Air Power's Cyber Risk: How Operational Causes will have Strategic Consequences

Word Count: 96,629

Submitted by Daniel Thomas Lydiate
to the University of Exeter as a thesis for the degree of
Doctor of Philosophy in Strategy and Security
January 2024

Acknowledgements

Academic research is filled with gratifying accomplishments and formidable trials. Amid the pursuit of knowledge, the summits consistently overshadow the troughs, making the expedition invariably worthwhile.

While my belief in this principle remains steadfast, my voyage as a doctoral student has illuminated the duality of unparalleled peaks alongside seemingly insurmountable challenges. This has been magnified by embarking on the odyssey as a part-time researcher separated by distance whilst also juggling the roles of husband, father, and Commissioned Officer. In this context, being surrounded by extraordinary individuals cannot be overstated.

Therefore, it is imperative to recognise that this scholarly exploration would have remained an unrealised aspiration without the support of my wife, Amy. Her boundless patience, unwavering encouragement, and incomprehensible understanding have been my bedrock.

Equally deserving of acknowledgment are my parents, Lindy and Derek. Their ceaseless guidance and meticulous proofreading have been invaluable.

Extending beyond this close ‘circle of understanding’, I offer my heartfelt thanks to the team at the Defence Science and Technology Laboratory (Dstl). Their early faith in my endeavour, continued funding, unwavering assistance, and profound expertise have been indispensable in enabling the inception, evolution, and fruition of this thesis.

Last but certainly not least, my gratitude goes to my supervisor, Dr David Blagden. From MStrat to Doctorate, his constant guidance has been a beacon, preventing me from straying off the scholarly path.

Abstract

This thesis argues that air power's cyber risk which has emerged from operational causes will create profound strategic consequences. Through a comprehensive examination of existing literature, it challenges prevailing perspectives by highlighting a critical gap in knowledge: a failure to map the link between operational causes and strategic consequences of air power's cyber risk which, when realised, will threaten the roles and, in extremis, survival of states. While acknowledging the risks emergent nature and situational specificity with not all states reliant on air power and size inverse to severity, the thesis asserts that the realisation of these strategic consequences is a matter of 'when', not 'if'. Developed within a risk management framework, supported by literature reviews and case studies, and leading to observations and recommendations, the thesis responds by offering a pathway for further research which can mitigate air power's cyber risk. If embraced, an opportunity exists for academia and practitioners to act in synergy, fill the identified gap in knowledge and address the risk proactively. Conversely, if ignored and the pathway is not followed, the implications will, the thesis predicts, result in the unmitigated strategic consequences of air power's cyber risk reshaping the geopolitical landscape of the 21st century.

Contents

Abbreviations

AAR	Air-to-Air Refuelling
ACA	Airspace Control Aircraft
ADIZ	Air Defence Identification Zone
AFFOC	Air Force Future Operating Concept
AFP	Advanced Forward Presence (NATO)
AI	Artificial Intelligence
ALOU	Autonomic Logistics Operating Unit
APT	Advanced Persistent Threats
APT1	Hacking group linked to the PLA (also referred to with the designator 61398)
ASPI	Australian Strategic Policy Institute
AT	Air Transport
AV	Anti-Virus
ATC	Air Traffic Control
ALIS	Autonomic Logistics Information System
ALOU	Autonomic Logistics Operating Unit
A2AD	Area Access / Area Denial
BALTNET	Baltic Air Defence Network
BREXIT	Britain’s Exit from the European Union
BRI	Belt and Road Initiative (PRC)
BUR	Bottom-Up Review (1993, US)
ARPANET	Advanced Research Project Agency Network (US)
CD	Compact Disc
CERT-UK	Computer Emergency Response Team – United Kingdom
CIA	Central Intelligence Agency (US)
CISA	Cybersecurity and Infrastructure Security Agency
CNA	Computer Network Attack
CND	Computer Network Defence
CNI	Critical National Infrastructure
CNO	Computer Network Operations
COIN	Counter-Insurgency (operations)

COPRI	Copenhagen Peace Research Institute
COTS	Commercial Off the Shelf
CPS	Cyber Physical Systems
CSA	Chief Scientific Adviser
CSCRM	Cyber Supply Chain Risk Management
CYBERCOM	Cyber Command (US)
C2	Command and Control
DCP	Defence Command Plan (UK)
DCS	Distributed Control System
DHS	Department of Homeland Security (US)
DfID	Department for International Development
DoD	Department of Defence (US)
DoS	Denial of Service
DOT&E	Director, Operational Test and Evaluation (US)
ECM	Electronic Counter Measures
EEZ	Exclusive Economic Zone
EFB	Electronic Flight Bags
EOTS	Electro-Optical Targeting System
EU	European Union
EW	Electronic Warfare
FAA	Federal Aviation Authority (US)
FBI	Federal Bureau of Investigation (US)
FCDO	Foreign, Commonwealth and Development Office
FCO	Foreign and Commonwealth Office
FIS	Foreign Intelligence Service
FoI	Freedom of Information
FOIP	Free and Open Info-Pacific
FoN	Freedom of Navigation
FRONTEX	European Union Border and Coast Guard Agency
FSB	Federal'naya Sluzhba Bezopasnosti (Russia)
FY	Financial Year
GCC	Ground Control Centre
GDP	Gross Domestic Product

GPS	Global Positioning Satellite
GRU	Glavnoe Razvedyvatel'noe Upravlenie (Russia)
GTsST	GRU’s 85th Main Centre for Special Technologies (Russia)
G8	Group of Eight
IAEA	International Atomic Energy Agency
IAF	Israeli Air Force
ICAO	International Civil Aviation Organisation
ICBM	Intercontinental Ballistic Missiles
ICEF	Information, Communication and Electronic Force
ICS	Industrial Control System
IDF	Indigenous Defence Fighter (Taiwan)
IDS	Intrusion Detection System
IHL	International Humanitarian Law
IMS	Integrated Maritime Surveillance
IMSC	International Maritime Security Construct
INSSG	Interim National Security Strategic Guidance (US)
IO	Information Operations
IOpC	Integrated Operating Concept (UK)
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IR	International Relations
IR	Integrated Review (UK)
IRA	Internet Research Agency (Russia)
IRBS	International Rules Base System
IRGC	Islamic Revolutionary Guard Corps (Iran)
ISIS	Islamic State of Iraq and Syria
ISR	Intelligence, Surveillance and Reconnaissance
ISTAR	Intelligence, Surveillance, Targeting and Reconnaissance
ISO	International Standards Organisation
IT	Information Technology
JADC2	Joint All-Domain Command and Control
JCPOA	Joint Comprehensive Plan of Action

JPO	Joint Program Office (US)
JSP	Joint Service Publication (UK)
KMT	Kuomintang (Chinese National Party, PRC)
LAN	Local Area Network
LoAC	Law of Armed Conflict
Malware	Malicious Software
MCA	Malicious Cyber Actor
MCI	Marine Corp Intranet (US)
MENA	Middle East and North Africa
MDI	Multi-Domain Integration
MITM	Man in the Middle
MI5	Domestic Security Services (UK)
MOD	Ministry of Defence (UK)
MOIS	Ministry of Intelligence and Security (Iran)
MRA	Mahak Rayan Afraz (Iran)
MRC	Major Regional Conflict
MSEB	Maharashtra State Electricity Board (India)
MT	Motor Tanker
NASA	National Aeronautics and Space Administration (US)
NATO	North Atlantic Treaty Organisation
NCSC	National Cyber Security Centre (UK)
NDAA	National Defense Authorisation Act (2022, US)
NDS	National Defense Strategy (US)
NextGen	Next Generation
NGAD	Next Generation Air Dominance (US)
NIST	National Institute for Science and Technology (US)
NORAD	North American Aerospace Defense (US)
NSA	National Security Agency
NOA	National Audit Office (UK)
NOAA	National Oceanographic and Atmospheric Administration
NSS	National Security Strategy (US)
OCTS	One Country, Two Systems (PRC)
ODC	Overall Defence Concept (Taiwan)

ODIN	Operational Data Integrated Network
ONG	Oil and Natural Gas
OPM	Office of Personnel Management (US)
OS	Operating System
OSI	Office of Special Investigation (USAF, US)
OSI	Open Systems Interconnection
OTE	Operational Test and Evaluation (Agency, US)
OT-1	Operational Test 1
PAC-3	Patriot Advanced Capability 3
PGM	Precision Guided Munitions
PHM	Prognostics and Health Management
PLA	People’s Liberation Army (PRC)
PLAAF	People’s Liberation Army Air Force (PRC)
PLAN	People’s Liberation Army Navy (PRC)
PRC	People’s Republic of China (PRC)
PWC	Price Waterhouse Cooper
P2P	Point to Point
QDR	Quadrennial Defense Reviews (US)
QEC	Queen Elizabeth-Class (aircraft carriers, UK)
QRA	Quick Reaction Alert
RAF	Royal Air Force (UK)
RAT	Remote Access Trojan
RCV	Robotic Combat Vehicle
RF	Radio Frequency
RM	Royal Marines (UK)
RMA	Revolution in Military Affairs
RN	Royal Navy (UK)
ROC	Republic of China (formal name for Taiwan)
RUSI	Royal United Services Institute
R2P	Responsibility to Protect
SAM	Surface to Air Missile
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management

SDR	Software-Defined Radios
SEAD	Suppression of Enemy Air Defences
SEATO	Southeast Asia Treaty Organisation
SLBM	Submarine Launched Ballistic Missiles
SOU	Squadron Operating Units
SR	Spending Review
SSF	Strategic Support Force (PRC)
SVR	Sluzhba Vneshnei Razvedki (Russia)
S&T	Science and Technology
STOVL	Short Take-Off and Vertical Landing
TA	Threat Alert
TAIPEI	Taiwan Allies International Protection and Enhancement Initiative Act (US)
Taipower	Taiwan Power Company
TTP	Tactics, Techniques and Procedures
UAD	User Access Devices
UAE	United Arab Emirates
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Air Vehicles
UK	United Kingdom
UN	United Nations
UNCLOS	UN Convention on the Law of the Sea
UNDP	United Nations Development Programme
UNSC	United Nations Security Council
US	United States
USAF	United States Air Force
USB	Universal Serial Bus
USD	United States Dollars
USIS	United States Investigation Service
USMC	US Marine Corp
USN	United States Navy
USS	United States Ship
USSBS	United States Strategic Bombing Survey

VPN	Virtual Private Network
WMD	Weapons of Mass Destruction
WMD	Western Military District (Russia)
WTO	World Trade Organisation
9/11	Terrorist attacks against the US mainland on 11 September 2001

Introduction

This thesis argues that though created through operational causes, air power's cyber risk will have the strategic state level consequences of a loss of role or, in extremis, survival. The assertion builds on an extensive body of existing literature at the operational and strategic levels. However, in examining this literature, the thesis challenges current thinking by identifying a distinct gap in knowledge that has been created by a failure to chart the causal relationship between the operational and strategic levels. This gap in knowledge, if not understood by academia and managed by practitioners, creates a risk that the maturing operational causes will act as a catalyst to the identified strategic consequences.

In highlighting this risk by asking how the operational causes of air power's cyber risk will have strategic consequences, the thesis sets out an unequivocal case for urgent action. Encapsulated in the observations and recommendations delivered in its concluding Part, an intellectual springboard is offered from which this action can be instigated, the gap in knowledge fully addressed and practical development achieved. Ultimately intending to inspire follow on research, the thesis is designed as a catalyst to initiate progress which will allow the causes of air power's cyber risk to be managed and its consequences mitigated to a point at which they become a footnote in history. If this development is not achieved the thesis warns that the risk will grow in the shadows of knowledge and predicts that the strategic impact will be severe. In such circumstances, those states who have come to rely on air power will see their socially constructed roles and even survival placed in jeopardy when the operational causes inevitably emerge as air power's cyber risk.

To ensure these arguments can be developed with depth, Part 1 of the thesis initially introduces the topic through an overview of the operational and strategic literature leading to confirmation on the identified gap in knowledge. With this established, Part 1 completes the foundational discussion by defining the overarching concept of cyber and introducing the International Relations (IR) theory which guides the research.

Building on this, the thesis in Part 2 confronts the question of why air power's cyber risk is strategic in nature by systematically exploring three identified causes: a reliance on air power by states with a global role or existential threat, the identification of pressing vulnerabilities and the emergence of viable threats. The strategic consequences that these causes create will then be articulated through a series of case studies in Part 3 which, though focused on Western and aligned powers, are asserted to offer universal relevance.

Leading to an assertion that it is a matter of 'when' not 'if' the strategic consequences of air power's cyber risk will emerge, the thesis finally in Part 4 summarises and offers clear observations and recommendations. It is within these that the gap in knowledge will be confirmed, the intellectual springboard crystallised, and the call for action if states are to be protected from the strategic consequences made.

To guide this discussion, and reach these conclusions with the rigour required, a robust methodology is essential. For the thesis, in both its research and delivery, this is founded in a risk management-based framework.

Emerging conceptually from the 'Compatibility Thesis', this methodological design was founded on the assessment that to engage with the real-world issue of air power's cyber risk the researcher must not be restricted by the limitations of positivism and interpretivism nor swayed by the arguments of the 'Incompatibility Thesis'[1]. Rather, it was judged that in line with the 'Compatibility

[1] For depth on research paradigms, see:

L.V Redman and A.V.H. Mory, *The Romance of Research* (Philadelphia: The Williams & Wilkins Company, 1933), iv.

C.R. Kothari, *Research Methodology: Methods and Techniques* (New Delhi: New Age, 2004), 8.

Y.S. Lincoln, *Handbook of Qualitative Research* (California: Sage, 1994), 163.

For depth on positivism and interpretivism, see:

C. Clarke, "Paths between Positivism and Interpretivism: An Appraisal of Hay's Via Media", *Politics,* 29, no. 1 (2009): 31.

Further comment on the 'Incompatibility Thesis' is as follows:

The 'Incompatibility Thesis' refers to the idea that different paradigms in the field of IR are fundamentally incompatible, and that there is no possibility for theoretical synthesis or reconciliation between them. This is because, as Burchill et al highlights, each of the IR paradigms are grounded in fundamentally different assumptions about the nature of international politics, and that these assumptions cannot be reconciled. This position has been supported by several prominent scholars including Waltz who suggested that attempts to reconcile different paradigms may lead to theoretical confusion, and Wendt who argued that different

Thesis' a methodological approach informed by analytical eclecticism which 'eschews rigid boundaries and hierarchies in the production of knowledge' must be embraced[2].

Recognising analytical eclecticism through this logic as an IR approach that seeks to combine insights and concepts from different perspectives to produce comprehensive understanding, its intent to avoid the limitations of a single theoretical approach was considered valuable. Though advocated by a breadth of scholars, prominently Keohane and Nye, it was noted that critics including Walt argue that such an approach creates theoretical inconsistencies[3]. Though Walt is supported by others including Little who contend that this type of 'smorgasbord' theory-building ignores underlying assumptions, by speaking to the multidisciplinary nature of real-world focused research it was concluded that the concept offered a convincing starting point[4].

Having emerged as a guiding light to the methodological design, adoption of these principles led to the identification of risk management as a pragmatic framework not limited by academic IR preconceptions. Though employed widely by cyber and air power practitioners alike to understand and manage the risk to operations, risk management enjoys little scholarly attention in IR. However, as IR 'grapples with the most recurrent risks of all', the synergies are notable[5]. Applying this logic, Jarvis and Griffiths argue that scholars can through risk

paradigms in IR are grounded in fundamentally different ontological assumptions. However, critics of this incompatibility position argue that it is based on a narrow and reductionist understanding of theory. For depth, see:

S. Burchill et al., *Theories of International Relations*, 3 ed. (Basingstoke: Palgrave Macmillan, 2005).

K.N. Waltz, *Theory of International Politics* (Reading MA: Addison-Wesley Publishing Company, 1979).

A. Wendt, "Anarchy Is What States Make of It: The Social Construct of Power Politics", *International Organization,* 46, no. 2 (1992).

[2] R. Sil and P.J. Katzenstein, *Beyond Paradigms: Analytic Eclecticism in the Study of World Politics* (Basingstoke: Palgrave MacMillan, 2010), 47.

[3] Scholars who have advocated for analytical eclecticism include:

R.O. Keohane and J.S. Nye, *Power and Interdependence*, 3 ed. (Boston Longman 2012).

E. Adler and M. Barnett, *Security Communities* (Cambridge1998).

Wendt, "Anarchy Is What States Make of It: The Social Construct of Power Politics".

For Walt's criticisms, see:

S.M. Walt, "The Renaissance of Security Studies", *International Studies Quarterly,* 35, no. 2 (1991).

[4] R. Little, "The Eclectic and Pragmatic Heritage of Ir Theory," in *Perspectives on World Politics* ed. R. Little and M. Smith (London: Routledge, 2006).

[5] D.S.L. Jarvis and M. Griffiths, "Risk and International Relations: A New Research Agenda?", *Global Society,* 21, no. 2 (2007): 2.

management replace uncertainty with quantifiable explanations[6]. Potentially either quantitative or qualitative depending on the risk framework adopted, the assertion speaks to evidencing scholarly arguments through evidence-based means. Aligning to the pragmatic approach eschewed by advocates including Morgenthau, risk management came into focus as the most suitable means of articulating and evidencing new knowledge with clarity[7].

Recognising the lack of focus on risk in IR, however, a requirement to build a bespoke framework became clear[8]. In resolving this, two points which articulate the final approach employed in the research are noteworthy[9]. Firstly, in line with the puzzle being addressed, a strategic level of risk consideration was chosen. Secondly, given this strategic level, a qualitative, not quantitative, approach was embraced[10]. In combination, a high-level narrative-based framework was adopted which guides the thesis through its development and delivery.

With the framework confirmed, it was recognised that for effective qualitative analysis a defined research methodology was necessary. Initially employing a breadth of secondary sources to understand the literature, primary research

[6] Jarvis and Griffith's argument is endorsed by Deuchars who contends that by replacing uncertainty with risk the world becomes more certain, and Clapton who concludes that 'riskisation' can identify and manage complex IR risks.

Ibid.

R. Duechars, *The International Political Economy of Risk: Rationalism, Calculation and Power* (London: Routledge, 2004), 2.

W. Clapton, "Risk in International Relations", *International Relations,* 25, no. 3 (2011): 281.

[7] H.J. Morgenthau, "The Hopelessness of Victory", *Foreign Affairs,* 32, no. 2 (1954).

[8] For a discussion on the under employment of risk management in IR, see:

Clapton, "Risk in International Relations", 292.

[9] Recognised risk management methodologies which were considered in the development of the methodology included:

ISO, "Iso/Ie 27005:2011 – Information Security Risk Management", (2011).

Information Security Forum, "Methodology 2 (Iram2)", (2019).

UK, "Hms Ia Standard Numbers 1 and 2: Information Risk Management", (2012).

National Institute of Standards and Technology, "Nist 800-30 – Guide for Conducting Risk Assessments", (2012).

UK, "The Orange Book: Management of Risk – Principles and Concepts", (2019).

[10] It is acknowledged that some consider qualitative risk considerations controversial. However, as 'risks are not concrete entities…which can be studied without subjective bias', and judgement is inherent to all forms of risk assessment, all risk management is ultimately qualitative in nature. Therefore, on balance, qualitative risk assessment at a strategic level is deemed suitable for this thesis.

For the quote, see:

B. Toft and S. Reynolds, *Learning from Disasters – a Management Approach* (Leicester: Perpetuity Press, 1997).

Examples of arguments against qualitative risk assessment include Hood and Jones who contend that quantitative risk management is the only effective way to expose anomalies and Adams who suggests that non-quantitative subjective assessments are merely 'air-fairy nonsense'.

C. Hood and D.K.C. Jones, *Accident and Design – Contemporary Debates in Risk Management* (London: Routledge Taylor and Francis Group, 1997), 1.

J. Adams, *Risk* (London: Routledge Taylor and Francis Group, 1994), 10.

Examples of support for the qualitative approach include:

N.R. Pidgeon, "Risk Perception within Risk – Analysis, Perception and Management", (Royal Society Study Group, 1992).

combined analysis of open-source intelligence, technical reports, and other grey literature to achieve a depth of understanding. In conducting the research in this manner it was recognised that the thesis would in large part shift away from traditional academic sources such as peer reviewed journals to sources that would routinely be treated with caution by the academic community. Though acknowledged, the emergent and cutting-edge technological nature of the research combined with its aim to fill an identified gap in academic knowledge meant that such open-source intelligence, technical reports, and other grey literature were pivotal.

To address the academic concerns which this extensive use of non-academically traditional sources created, all were robustly considered against Scotts' research criteria of authenticity, credibility, representativeness and meaning[11]. By doing so systematically at every stage of the research, and by reflecting on the limitations of each source in the context it was being read, a research pathway was forged which did not undermine the academic basis. Rather, in taking this approach, depth and clarity were added to the argument, and the thesis was able to uniquely fill an identified gap in knowledge. In doing so, the arguments were enriched allowing the final offering to generate greater value to both the academic and practitioner communities[12].

In a final element of the research design the ethical perspective was explored. In this, the University of Exeter ethics procedures and, due to the source of funding, the MOD Research Ethics Committee (MODREC) were considered. Given the nature of the research and methodology employed, it was confirmed that neither were required to be pursued[13].

[11] J.A. Scott, *Matter of Record* (Cambridge: Polity Press, 1990).

[12] For further discussion on the management of non-traditionally academic sources, see:
P. McNeill and S. Chapman, *Research Methods* (London: Routledge, 2005).

[13] For the University of Exeter research ethics policy, see:
University of Exeter, "Research Ethics Policy and Framework", (2021).
The PhD was funded by the Defence Science and Technology Laboratory (Dstl). For the MODREC ethics policy, see:
UK, "Ministry of Defence Research Ethics Committee", ed. Ministry of Defence (2022).
"Jsp 536 - Defence Research Involving Human Participants", ed. Ministry of Defence (2022).

Having introduced the overarching argument, and outlined the research methodology, the thesis will now in Part 1 confirm the gap in knowledge and explore the founding concepts. Building on these, the risk management methodology will unfold in Parts 2 and 3 before the conclusions, observations and recommendations of Part 4 offer the intellectual springboard. This springboard, if used, will address the gap in knowledge and ensure air power's cyber risk does not become a defining factor of the 21st century.

Part 1: The Foundational Concepts

Chapter 1: Supporting Literature and the Gap in Knowledge

Introduction

To open this discussion of how the operational causes of air power's cyber risk will have strategic consequences this chapter provides a foundation by summarising the digitisation of air power. Building on this, it will then explore the literature upon which the thesis is built and identify an existing gap in knowledge. In doing so the necessity to conduct further research and chart the 'golden thread' between the operational causes and strategic consequences of air power's cyber risk will be demonstrated.

The Digital Enablement of Air Power

In commencing this discussion, it is first necessary to understand how this gap in academic knowledge has come into being through the digital evolution of air power. This process of digitisation has become central to the operation of air power and led the capability to be increasingly entwined with the military instrument of power[14].

To fully appreciate this development, it is necessary to initially look back to the Cold War and a requirement for robust communications[15]. Leading by 1969 to the first resource-sharing network, such early offerings provided advantage but were limited by a requirement for fixed sites[16].

[14] The instruments of national power are routinely defined as diplomatic, military, and economic. For Governmental and academic discussion of the instruments, see:

"Joint Defence Doctrine 0-01 Uk Defence Doctrine", ed. Defence Concepts and Doctrine Centre (: Ministry of Defence, 2014).

D. Jablonsky, "National Power", *Parameters,* Spring (1997): 55.

J.S. Nye, "Get Smart: Combining Hard and Soft Power", *Foreign Affairs,* 88, no. 4 (2009): 160.

J.J. Mearsheimer, *Structural Realism' in International Relations Theories: Discipline and Diversity* (Oxford: Oxford University Press, 2007), 72.

[15] J. Naughton, "The Evolution of the Internet: From Military Experiment to General Purpose Technology'", *Journal of Cyber Policy,* 1, no. 1 (2016): 7.

[16] This was the US Advanced Research Project Agency Network (ARPANET) which would grow to nearly 60 nodes by the mid-1970s.

B. Tarnoff, "How the Internet Was Invented", *The Guardian* 15 July 2016.

Gaining momentum in line with the development of civilian technologies, military digitisation was by the 1990s hailed as a Revolution in Military Affairs (RMA)[17]. Though this title has been challenged, there was in this period a clear transition from platform-centric to network-centric warfare[18]. A prominent example was the 1996 Straits of Taiwan crisis. A showdown between the US and the PRC over Taiwanese democratisation, the crisis witnessed the US Navy (USN) harness network enabled technologies to deploy a carrier group in a matter of hours rather than the pre-digital timescale of days[19].

Building from the late 1990s, the military reliance on digital networks has now reached a point at which there are no longer any elements of operations conducted purely in the physical space[20]. Rather, as UK military doctrine comments, it is the interplay between cyber and kinetic effects that define contemporary operations[21].

Though offering obvious advantage, some have warned that with militaries now 'as reliant on fast network connections as [they are] on breathable air' any loss or compromise of this cyber enablement will mean the loss of operational effectiveness[22]. A concern for all elements of the military lever of power, this over-reliance and its associated risk is arguably enhanced for air power. Whilst, for example, an infantry soldier might lose situational awareness, rifles continue to

[17] For a discussion on the increasing momentum of cyber within the military instrument of national power see:
R. Cohen-Almagor, "Internet History", *International Journal of Technoethics,* 2, no. 2 (2011).
For a discussion which extends the concept of digitisation being classed as a RMA, see:
A.K. Cebrowski and J.J Garstka, "Network-Centric Warfare: Its Origin and Future", *US Naval Institute Proceedings,* 124, no. 1 (1998): 29.

[18] For an example of challenge, see:
M.C. Libicki, "Why Cyber War Will Not and Should Not Have It Grand Strategist", *Strategic Studies Quarterly,* 8, no. 1 (2014): 24.
For a discussion of this transition, see:
J. Johnson, interview by R. Steinnon, 7 December 2017.

[19] For further background on the 1996 Straits of Taiwan crisis, see:
R.S. Ross, "The 1995-96 Taiwan Strait Confrontation: Coercion, Credibility and the Use of Force", *International Security,* 25, no. 2 (2000): 95.
For a discussion of the role of technology in the crisis, see:
Cebrowski and Garstka, "Network-Centric Warfare: Its Origin and Future", 34.

[20] This argument for the pervading nature of cyber in contemporary operations is made in UK Military doctrine, specifically Joint Concept Note (JCN) 2/17 (2017).
UK, "Joint Concept Note (Jcn) 2/17 – Future of Command and Control", ed. Ministry of Defence (2017), 4.

[21] Ibid.

[22] The quote is taken from the Armed Forces Journal's discussion on military reliance of digital networks and systems. This view was underlined by General Mattis, a former USMC General and US Defence Secretary, who commented in 2014 that US forces were no longer able to operate 'when [digital] systems go down'.
Staff-Writer, "Practice Disconnected", *Armed Forces Journal,* (2012).
J.N. Mattis, interview by S. Beauchamp, 29 November 2014.

operate without digital support. However, with all advanced air power reliant on 'timely, accurate and untampered information' the compromise of its cyber environment would logically have a far greater impact[23].

This reality, which will be discussed in more depth as the thesis progresses, can be realised through all the people, infrastructure, and systems elements of cyber introduced in Chapter 2. However, to appreciate the crux of its occurrence and the central importance of cyber to air power, it is intuitive to initially focus on digital systems and networks.

Though in this area air power's reliance on digitisation does not differ in principle from other cyber enabled environments, aviation does offer a notably complex example. Epitomised by Next Generation (NextGen) technologies, multiple networks are now interconnected aboard single air platforms[24]. Leading flight to be increasingly autonomous, innovations have shifted aviation away from the human-centric concept of a pilot controlling an aircraft to digital management. Examples which personify this include voice communications which are no longer the primary source of information in flight, and Cyber Physical Systems (CPS) which actively monitor and control the physical processes previously conducted by people[25].

[23] R. De Cerchio, "Aircraft Systems Cyber Security", in *Digital Avionics Systems Conference (DASC)* (2018), 2.

[24] For discussions of NextGen technologies in aviation, see:
Ibid.
M. Yeh, J. Jaworski, and S. Chase, "Pilot Perceptions on the Integration of Electronic Flight Bag Information in New Flight Deck Designs", in *Human Factors and Ergonomics Society Annual Meeting* (2019).
US, "Modernizing Us Air Space: Next Generation Air Transportation", ed. Federal Aviation Authority (2020).

[25] For a discussion of digitised systems being the primary source of information in flight, see:
De Cerchio, "Aircraft Systems Cyber Security", 3.
For aviation reliance on CPS, see:
Ibid.
Staff-Writer, "The Future of Automoation in the Aviation Industry", *Robotics & Automoation,* (2019).
E.A. Lee, "Cyber Physical Systems: Design Challenges", in *Technical Report No. UCB/EECS-2008-8 - Electrical Engineering and Computer Sciences* (University of California at Berkeley, 2008).
For the dangers of relying on CPS citing the 2019 crashes of the Boeing 737 Max 8 aircraft, see:
J. Nicas and Z. Wichter, "A Worry for Some Pilots: Their Hands-on Flying Skills Are Lacking'", *The New York Times*, 14 March 2019.
T. Harford, "Crash: How Computers Are Setting Us up for Disaster", *The Guardian*, 11 October 2016.
S. Baker, "The Boeing 737 Max Crashes Have Revived Decades Old Fear About What Happens When Airplane Computers Become More Powerful Than Pilots", *Business Insider*, 17 February 2020.
M.L. Olive, R.T. Oishi, and S. Arentz, "Commercial Aircraft Information Security - an Overview of Arnc Report 811", in *25th Digital Avionics Systems Conference* (2006).

The result has been the air power cyber environment, and the digital information within it, becoming the 'life blood' of air operations[26]. Recognising this, those entrusted with operating air power are presented with a pressing requirement to assure the 'timely, accurate and untampered' nature of digital information[27]. However, with the combination of multiple complex networks and systems now extensive, and every data exchange, no matter how small, offering a potential for compromise, identifying, and managing air power's cyber advantages and its cyber risks has become a significant challenge[28].

In the first, air power's cyber advantages, we see echoes of the capability's development since its initial strategic use in 1915[29]. Routinely characterised as harnessing cutting-edge technologies to achieve advantage over an adversary, air power's strengths have for over a century made it a decisive factor in virtually all conflicts[30]. Continuing into the 1990s, this trend took a step forward through the advances offered by the cyber environment. Allowing enhancements from communications through to intelligence gathering and precision guided munitions, air power has through cyber enablement been able to deliver increased impact, at distance with a relatively small number of assets[31].

[26] The concept of information being the 'lifeblood' of aviation is borrowed from other sectors. In Defence for example UK Doctrine asserts that information has become the lifeblood of delivering operations. Equally, in business information is described by Ghasemkhani et al (2015) as 'the lifeblood of organisations, which absorb, generate, transform and share information continuously'. Though just two examples, they highlight how information has in the modern world become imperative to all industries including, it is asserted, air power.

UK, "Joint Service Publication (Jsp) 441 – Managing Information in Defence – Part 1: Directive", (Ministry of Defence 2017).

H. Ghasmekhani, D. Soule, and G. S. Westerman, "Competitive Advantage in a Digital World: Toward an Information-Base View of the Firm", (SSRN, 2015).

[27] For quote, see:

De Cerchio, "Aircraft Systems Cyber Security", 2.

[28] This characterisation of the vulnerability of digital systems is made by the US Operational Test and Evaluation (OTE) Agency. For depth, see:

US, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs: Memorandum for Commander Army Test and Evaluation Command and Air Force Operational Test and Evaluation Centre", ed. Operational Test and Evaluation (2014).

[29] The strategic use of military air power is considered to have been pioneered during World War One with the German use of Zeppelin Airships to attack Britain on 19-20 January 1915. At this time, however, air power was considered a minor capability with limited strategic effect.

C. Stephenson, *Zeppelins: German Airships 1900?* (Oxford: Osprey Publishing, 2005), 13.

[30] For arguments of air power being a strategically decisive capability, see:

B.S. Lambeth, *American Air Power* (London: RAND, 2000), 8.

R. Frankum, *Like Rolling Thunder: The Air War in Vietnam, 1964-1975*, vol. 3 (New York Rowman & Littlefield, 2005), 75.

C. Posey, "Air War in the Falklands", *Air and Space Smithsonian,* 17, no. 3 (2002): 75.

[31] B.S. Lambeth, *The Transformation of American Air Power* (Ithica: Cornell University Press, 2000), 236.

R.A. Pape, "The True Worth of Air Power", *Foreign Affairs,* 83 (2004): 16.

With momentum maintained into the 21st century, these advantages became increasingly pronounced. A prominent example is the advent of 'Fifth Generation' aircraft which harness technology to a point at which air platforms are integrated with, and therefore fully exploiting, their digital networks[32]. When employed operationally, these offer considerable advantage over adversaries through the delivery of multi-role capabilities and the exploitation of real-time digital feeds[33]. Translated into strategic effect, states can rely on a relatively small fleet of aircraft to achieve impact across numerous defence tasks. In doing so, air power has for many states become keystone to maintaining the role to which they aspire.

Beyond this evolution, Unmanned Aerial Vehicles (UAV) have also begun to redefine how air power can exploit the cyber environment. Whilst in some circumstances UAVs retain a human controller at distance, they are still operated entirely through their digital systems and networks. Heavily invested in, the role these autonomous platforms play continues to be extended. In doing so, states have begun to maximise the strengths of air power whilst mitigating its traditional limitations incurred, in large part, because of the fragilities of the human pilot[34].

Taken collectively, it is evident that cyber enablement will continue to both dominate air power and enshrine its position as a preeminent military strategic capability[35]. Notwithstanding this, it is also evident that by embracing the cyber environment air power has become exposed to considerable new cyber risk.

[32] '5th Generation' aircraft represent the culmination of a century of development. Building on advances from the 'zeroeth Generation's' first use of jet engines through to the '4th Generation's' improvements in avionics, '5th Generation' aircraft initially entered service in 2015 in the form of the F-35. Now joined by China's J-20 and Russia's Su-57, their defining characteristic is a significant advancement in information systems and associated software. For depth, see:
Staff Writer, "Five Generations of Jets ", *Fighter World*2018.
F. Gady, "China's First Fifth Generation Fighter Jet Is Operations", *The Diplomat,* (2017).

[33] The F-35 can be cited as an example of these advantages. For depth, see:
LockheedMartin, "About the F-35: The Multi-Variant, Multirole 5th Generation Fighter", (2020).
A. Norman, interview by D. Martin, 2014.
S. Roblin, "Can China's Chengdu J-20 Stealth Fighter Win against America's F-35 or F-22", *National Interest*, 14 September 2019.

[34] K. Hartmann and C. Steup, "The Vulnerability of Uavs to Cyber-Attacks; an Approach to the Risk Assessment", in *Cyber Conflict (CyCon) 5th International Conference* (2013), 1.

[35] The assertion that air power is a preeminent strategic capability is based on the evidence that it has been consistently employed by advanced states as a mainstay of the military lever of power since the Second World War. For examples and depth, see:
ICAO, "Airspace Sovereignty", in *ICAO Worldwide Air Transport Conference* (2013).
A.J. Williams, "A Crisis in Aerial Sovereignty? Considering the Implications of Event Military Violations of National Airspace", *Area,* 42, no. 1 (2010).
NATO, "Hungary to Lead Nato's Baltic Air Policing, Joined by Uk and Spain ", (2019).
A.L. Johnson, *Wars in Peace: British Military Operations since 1991* (London: RUSI, 2014).
Stephenson, *Zeppelins: German Airships 1900?* .

Manifested through the vulnerabilities of digital systems, this risk is realised by the threat of hostile actors exploiting the cyber environment. Freeing adversaries from physical limitations, this allows actors through non-conventional means to target air power and achieve strategic impact at distance[36]. An option not only open to states but state-sponsored and non-state actors, the result is a form of digital asymmetric conflict which is placing air power at increasing risk[37].

The Operational Literature: The Causes of Air Power's Cyber Risk

The above narrative illustrates how through its digital evolution there is a strong argument that a unique cyber risk now threatens the viability of air power. However, this issue can, and must, be further analysed in terms of both its operational causes and strategic consequences. Delivered in depth through the iterative parts of this thesis, it is necessary before commencing this discussion to confirm that sufficient literature is offered to explore this topic with the necessary rigour. Within this, it is logical to begin at the operational level.

Discussed in depth in Parts 2 and 3, this literature offers prime examples of the sources available to the academic researcher. Emerging from the kernel of Moore's Law which in 1965 accurately predicted that digital processing power will on average double every two years, academics have at an operational level in the interceding six decades actively charted the development of technology and its impact on not only warfare but air power[38]. To consider this literature, one must first reflect on how cyber vulnerabilities to air power have been discussed through three core elements that will be revisited later in the thesis: the people who operate air power, the digital information it relies on and the infrastructure through which it is delivered.

R.A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithica: Cornell University Press, 1996).
K. Payne, *Deterrence in the Second Nuclear Age* (Lexington Kentucky University Press, 1996).

[36] As Nye comments, in the virtual world of cyber 'physical distance is immaterial'. Therefore, where an actor might previously have been prevented from targeting assets due to the limitation of physical distance, cyber attacks (assuming assets are networked and connected to the internet) allow the removal of this restriction and the mounting of attacks at distance.
J.S. Nye, *Cyber Power* (Cambridge, MA: Harvard University Press, 2010).

[37] A. Granova and M. Slaviero, "Cyber Warfare," in *Computer and Information Security Handbook*, ed. J.R. Vacca (Burlington: Morgan Kaufmann, 2017).

[38] G.E. Moore, "Cramming More Components onto Integrated Circuits", *Electronics,* 38, no. 8 (1965).

In terms of the people, the academic exploration of this human element at an operational level is significant but varied. From one perspective, for example, an intuitive discussion might be how cyber risk will emerge via the full automation of air platforms. Though explored, the predominance of academics argue that though technology will in time replace the human pilot it is not yet evolved enough[39]. Therefore, whilst there are sources on the emergence of true Artificial Intelligence (AI) in air power, it remains largely the purview of futurology making it of limited value to the real-world focus of this thesis.

Alternatively, an aspect of the people discussion which is found to be both of value and deeply researched is that of the 'insider threat' and how it may undermine air power. Referring to those with legitimate digital access to an organisation's sensitive material, and who may use this access to introduce risk to air power, significant general academic explorations include Crowdy's *The Enemy Within and* Homoliak et al's *Insight into Insiders and IT?*[40]. With more focused offerings from academics including Hochberg et al or Bunker and Fielding, all of which act to underline Moschovitis' 'people singularity' which contends that people remain the single most prevalent cyber risk for all digitally enabled industries, there is a depth of literature on this topic[41]. Whilst not all are air power centric, the wider body has direct relevance. This argument is illustrated by psychological explanations offered by Nurse et al and John et al, or specific models of behaviour such as those offered by Goldberg or Paulhus and Williams'. Notably, all combine to deliver a clear understanding of why insiders form a credible operational risk to a digitally reliant air power[42].

[39] For a representative example of this discussion, see:
K. Dear, "Artificial Intelligence and Decision-Making", *The RUSI Journal,* 164, no. 5 (2019).

[40] T. Crowdy, *The Enemy Within* (London: Bloomsbury, 2011).
I. Homoliak et al., "Insight into Insiders and It: A Survey of Insider Threat Taxonomies, Analysis, Modelling and Countermeasures", *ACM Computing Surveys,* 99 (2019).

[41] J. G. Hochberg et al., "Addressing the Insider Threat", in *The DOE Computer Security Group Conference* (1993).
C. Moschovitis, "Why So Cyber Security Programmes Fail?", *Cyber Security,* 2, no. 4 (2019).

[42] J. R. Nurse et al., "Understanding Insider Threat: A Framework for Characterising Attacks", *Security and Privacy Workshops,* (2014).
P.O. John, S.E. Hampson, and L.R. Goldberg, "The Basic Level in Personality-Trait Hierarchies: Studies of Trait Use and Accessibility in Difference Contexts", *Journal of Personality and Social Psychology,* 60, no. 3 (1991).
L.R. Goldberg, "The Structure of Phenotypic Personality Traits", *American Psychologist,* (1993).
D.L. Paulhus and K.M. Williams, "The Dark Triad of Personality: Narcissism, Machiavellism and Psychopathy", *Journal of Research in Personality,* 36 (2000).

This solid foundation for analysis of the operational level is further enhanced when considering the digital information air power relies on to operate. Though due to the cutting-edge nature of this topic a predominance of the information is taken from primary technical sources such as reports produced by the US Operational Test and Evaluation (OTE) Agency, and industry publications such as *Aviation Today,* it remains clear that significant valid albeit not academically peer-reviewed research has been conducted[43].

Further, when exploring the academic literature in this area the sources are notably specialist peer reviewed journals including the *Journal of Aerospace Engineering and Technology* or conference papers from sources such as the *Aerospace Conference.* Though notably outside the traditional perview of IR research, when taken collectively with relevant books on the topic and the aforementioned technical reports and industry publications, a significant depth of understanding is offered.

This is again reflected when considering the infrastructure on which digitally enhanced air power relies. Beginning with overarching offerings such as Cornish et al’s exploration of the cyber threat to Critical National Infrastructure (CNI), and adding depth through examples such as Chee-Wooi et al’s more technical discussion on CNI attack and defence modelling, the breadth of academic literature at an operational level in this area is significant[44]. Augmented in media and industry discussions with specific case studies such as the 2015 cyber attack on the Ukrainian power grid which bring the theoretical into real-world focus[45],

[43] For an example of an OTE Agency report used in the research, see:
US, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs: Memorandum for Commander Army Test and Evaluation Command and Air Force Operational Test and Evaluation Centre".
For an example of an industry publication on the digital information air power relies on, see:
C. Biesecker, "Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, Dhs Says", *Aviation Today*, 8 November 2017.

[44] P. Cornish et al., "Cyber Security and the Uk’s Critical National Infrastructure", *A Chatham House Report,* (2011).
T Chee-Wooi, G. Manimanran, and Liu C., "Cybersecurity for Critical Infrastructures: Attack and Defense Modelling", *IEEE Transactions on Systems: System and Humans,* 40, no. 4 (2010).

[45] For examples of media, industry, and governmental discussion of the events in 2015, see:
TCH, "Due to a Hacker Attack, the Power of Half the Ivano-Frankivsk Region Was De-Energised", TCH Online, https://translate.google.co.uk/translate?hl=en&sl=ru&u=https://ru.tsn.ua/ukrayin a/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti550406.html&prev=search.
UK, "National Cyber Security Strategy", ed. Cabinet Office (HM Government 2016).
US, "Alert (Ir-Alert-H16-056-01), Cyber-Attack against Ukrainian Critical Infrastructure", ed. Department of Homeland Defence (International Control Systems Computer Emergency Response Team, 2016).
D.U. Case, "Analysis of the Cyber-Attack on the Ukrainian Power Grid", *Electricity Information Sharing and Analysis Centre (E-ISAC)*, no. March (2018).

the ability to make assessments of the causes of air power's cyber risk in the operational space are clear.

Moving focus from the operational vulnerabilities which contribute to air power's cyber risk to the threats that target them, industry and open-source Government publications emerge as increasingly relevant. However, academically traditional sources remain a strong factor in building the argument. For example, in discussing cyber power and influence academic sources are heavily relied on to create understanding[46].

This theme is notably prevalent in the 'sea change' experienced through the impact of digitised technology. Articulating a contemporary evaluation of cyber power and how it may manifest in air power's cyber risk, sources including Nye's *Cyber Power,* Kuehl's *From Cyberspace to Cyber Power* and Willet's *Assessing Cyber Power* develop the discussion[47]. When wrapped into Hart's more traditional understanding of power, the importance of this academic foundation on why cyber power manifests, how it becomes influential and why actors will harness it to undermine air power is evident[48].

In turning to the practical application of how cyber actors will in practice harness this influence through tangible cyber threats, academic sources remain relevant, but the balance begins to shift towards a greater focus on industry publications. For example, in explorations of cyber threats in hybrid warfare academic sources form a key theme[49]. However, the balance shifts in the more refined discussions

[46] For examples of academic sources of cyber power and influence, see:

P. Deane, *The First Industrial Revolution* (Cambridge Cambridge University Press, 1979).

M. Haradhan, "The Second Industrial Revolution Has Brought Modern Social and Economic Developments", *Journal of Social Sciences and Humanities,* 6, no. 2 (2020).

D. Lyon, "From 'Post-Industrialism' to 'Information Society: A New Social Transformation? ", *Sociology,* 20, no. 4 (1986).

J. Riftkin, "Leading the Way to the Third Industrial Revolution", *European Energy Review,* 1 (2008).

K. Schwab, *The Fourth Industrial Revolution* (New York: Crown, 2016).

[47] J. Arquilla and D. Ronfeldt, "Cyberwar Is Coming!", *Comparative Strategy,* 12, no. 2 (1993).

Nye, *Cyber Power*.

M. Willett, "Assessing Cyber Power", *Survival,* 61, no. 1 (2019).

D.T. Kuehl, "From Cyberspace to Cyber Power: Defining the Problem," in *Cyberpower and National Security* ed. F.D. Kramer, S. Starr, and L.K. Wentz (Washington, D.C.: National Defense, 2009).

[48] J. Hart, "Three Approaches to the Measurement of Power in International Relations", *International Organisation,* Spring (1976).

[49] For examples of academic discussions on hybrid warfare, see:

of the cyber threat to air power with the value of media and industry offerings coming to the fore alongside supporting academic sources[50].

Taken as a whole, it is evident that there is through the combination of academic, governmental, industry and media sources a considerable basis for the study and assessment of the operational level causes of air power's cyber risk. Whilst many of these sources are not air power specific, the commonalities between digital industries ensures, as will be demonstrated in the arguments presented in Parts 2 and 3, that at an operational level air power's cyber risk can be explored, discussed, and confirmed through a significant depth and diversity of resources.

The Strategic Literature: The Consequences of Air Power's Cyber Risk

At an operational level, the above summary confirms that across academic, industry, governmental and media literature there is extensive resources upon which the research can be conducted. This continues into the strategic level consequences of air power's cyber risk.

Considering first the concept of cyber as a strategic level influencer, academic and wider think tank discussions on how the digital environment has evolved as

P.J. Cullen and E. Reichborn-Kjennerud, "Understanding Hybrid Warfare", *Multinational Capability Development Campaign (MCDC),* (2017).
P.R. Mansoor, "Hybrid War in History," in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* ed. M. Williamson and P.R. Mansoor (Cambridge Cambridge University Press, 2012).
V. Gerasimov, "The Value of Science Is in the Foresight", *Military Review,* (2016).

[50] For examples of industry sources, see:
Norton, "Malware – What Is a Trojan? ", (2020).
US, "Understanding Denial-of-Service Attacks', Security Tips", ed. Cyber-Security & Infrastructure Agency (2009).
NIST, "Cyber Supply Chain Risk Management", (National Institute of Standards and Technology 2020).
For examples of media sources, see:
A.K. Garg, "Fourth Generation Systems and New Wireless Technologies," in *Wireless Communications and Networking*, ed. A.K. Garg (Burlington: Morgan Kaufmann, 2007).
S. Boyson, "Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical It Systems", *Technovation,* 34 (2014).
For examples of academic sources, see:
D. Horschig, "Cyber-Weapons in Nuclear Counter-Proliferation", *Defense and Security Analysis,* 36, no. 3 (2020).
C. Kapan, "Air Power's Visual Legacy: Operation Orchard and Aerial Reconnaissance Imagery as Resus De Geurre", *Critical Military Studies,* 1, no. 1 (2015).
S. Quinian, "Jam. Bomb. Hack? New Us Cyber Capabilities and the Suppression of Enemy Air Defences", *Georgetown Security Studies Review,* (2014).
F.A.B. Da Silva, D.F.C. Moura, and J.F. Galdino, "Classes of Attacks for Tactical Software Defined Radio", *International Journal of Embedded and Real-Time Communication Systems,* 3, no. 4 (2012).
K. Hartmann and K. Giles, "Uav Exploitation: A New Domain for Cyber Power", in *8th International Conference on Cyber Conflict* (NATO CCDCOE 2016).
B. and Ly Ly, R., "Cybersecurity in Unmanned Aerial Vehicles (Uavs)", *Journal of Cyber Security Technology,* (2020).

a tool of strategic power and influence are significant. Explored by academics including Willett and Nye and codified in examples including the Belfer Centre's *National Cyber Power Index,* this literature offers an understanding of how the use of digital means in a cyber domain are already impactful and will be more so in the future[51]. Added depth by supporting quantitative assessments of cyber power and challenged by qualitative conceptualisations such as those explored by Betz and Stevens, there is a deep strategic level narrative on the nature and harnessing of cyber power to achieve influence[52].

These discussions are offered further context through wider, valuable but more theoretical explorations of the potential impact of cyber as a tool of national power. A discussion routinely considered to be rooted in Arquilla and Rondsfelt's 1992 *Cyber War is Coming!,* and notably developed by Rid's 2012 *Cyberwar Will not Take Place,* this exploration has evolved significantly over the last three decades[53]. For example, Rid argued that 'cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future'[54].

Reflecting on this, Rid's assertions could lead to a conclusion that cyber threats have not evolved to the point at which they could meaningfully impact air power or, therefore, have strategic influence. This is supported by the *Tallinn Manual,* NATOs attempt to codify conduct in the cyber domain, which in 2013 commented that no cyber events had ever met the criteria of 'war'. Though in drawing this conclusion the Manual acknowledges that the Stuxnet virus had come close, one

[51] Nye, *Cyber Power*.
Willett, "Assessing Cyber Power".
J. Voo et al., "National Cyber Power Index 2020", (Belfer Center, 2020).

[52] For examples of other quantitative modelling of cyber influence at a strategic level, see:
ITU, "Global Cybersecurity Index, Version 4 ", (International Telecommunications Union 2018).
M. Hathaway, "Cyber Readiness Index 2.0: A Plan for Cyber Readiness", (Potomac Institute for Policy Studies, 2015).
Economist-Intelligence-Unit, "Cyber Power Index", (Booz Allen Hamilton 2011).
For Betz and Stevens' qualitative modelling of cyber influence, see:
D.J. Betz and T. Stevens, *Cyberspace and the States: Toward a Strategy for Cyber-Power* (Abingdon: Routledge, 2011).

[53] Arquilla and Ronfeldt, "Cyberwar Is Coming!".

[54] For Rid's argument, see:
T. Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies,* 35, no. 1 (2012).
For Clausewitz definition of an 'act of war', see:
C. Clausewitz, *On War* (New Jersey: Princeton University Press, 1832).

might suggest that the current literature undermines any understanding of cyber as relevant at the strategic level.

However, as will be explored in the thesis, Rid links potential strategic impact of cyber to the Clausewitzean definition of an 'act of war'[55]. With a significant combination of academic, governmental and wider media comment predicting events akin to a 'cyber Pearl Harbour', a weight of literature has been created which not only underlines the emergent strategic importance of cyber as a domain but ensures it is supported by a significant body of thought[56].

Having outlined the existing literature on cyber at a strategic level, the next area to consider is air power itself as a tool of national power. Specifically, it must be ascertained whether there is sufficient literature to justify the assertion that air power is a principal military capability which if lost or compromised may undermine the strategic role or even survival of states.

Addressed in depth in the discussion of the procurement and reliance on digitally enhanced air power, it is shown that the body of literature is extensive. Building on Hart's explanation of how power achieves influence, this literature can be logically explored in terms of how power is harnessed across the categories of hard, soft, and smart[57].

[55] Rid, "Cyber War Will Not Take Place", 1.

[56] For the 'Cyber Pearl Harbour' quote, see:
L.E. Panetta, interview by E. Bumiller and T. Shanker, 11 October 2012.
For examples of discussions on the importance of cyber as a domain in the strategic sense, see:
M.C. Libicki, "Cyberspace Is Not a Warfighting Domain", *ISJLP,* 82 (2013).
R.A. Clarke and R.K. Knake, *Cyber War* (New York: Ecco, 2010).
M.N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).
M.N. Schmitt and B.T O'Donnell, "Foreword – Computer Network Attack and International Law", *International Law Studies,* 76 (2002).
R. Ottis, "Analysis of the 2007 Cyber-Attacks against Estonia from the Information Warfare Perspective", in *7th European Conference on Information Warfare* (2004).
Wheeler, "In Cyberwar, There Are No Rules: Why the World Desperately Needs Digital Geneva Conventions", *Foreign Policy,* (2018).
P. Withers, "What Is the Utility of the Fifth Domain?", *Air Power Review,* 18, no. 1 (2015).
B. Lilly and J. Chersvitch, "The Past, Present and Future of Russia's Cyber Strategy and Forces", in *12th International Conference on Cyber Conflict* (Tallinn NATO CCDCOE, 2020).
Gerasimov, "The Value of Science Is in the Foresight".

[57] For Hart's model, see:
Hart, "Three Approaches to the Measurement of Power in International Relations".
For discussions on how power can be categorised as hard, soft, and smart, see:
J. S Nye, "Public Diplomacy and Soft Power", *The Annals of the American Academy of Political and Social Science,* 616, no. 1 (2008).

Focusing on air power specifically, and considering its hard power utility, the literature again continues to be significant. Building from the early use of air power in the First World War, through its evolution in the Second World War to its employment through the 20th century, academic examinations of air powers hard power utility offer a depth of resource[58]. When underpinned by the lineage of air power scholars from Douhet through to Warden, the academic evidence for the utility of air power in a hard power role offers the researcher all the resource required to develop the argument on the relevance of the capability to the strategic role and survival of states[59].

Considering next soft power, the linkage is not as direct, but there remains a significant body of literature to support the utility of air power. Building from an understanding of soft power as offered by academics including Nye, and considering how as discussed by McClory soft power is ranked, this utility can be explored through a variety of literature[60]. With a framework to this discussion provided by Lowther's concept of 'air diplomacy', it becomes evident that whether in terms of humanitarian support, public engagements or capacity building the literature proves how air power's utilities of speed and reach allow it to outperform the military domains of land and sea in the delivery of strategic relevance[61].

[58] For an example of an examination of First World War air power, see:
Stephenson, *Zeppelins: German Airships 1900?* .
For an example of an examination of Second World War air power, see:
B.L. Montgomery, "The Role of Science in Warfare of the Future", *Engineering and Science* 18, no. 3 (1954).
For examples of examinations of the use of air power in the 20th century, see:
Vietnam War:
Frankum, *Like Rolling Thunder: The Air War in Vietnam, 1964-1975*, 3.
Falkland War:
Posey, "Air War in the Falklands".
Gulf War:
R.P. Hallion, *Storm over Iraq: Air Power and the Gulf War* (London: Smithonian Books, 1997).
Libyan intervention:
K.P. Mueller, *Precision and Purpose: Airpower in the Libyan Civil War* (Santa Monica: RAND, 2015).
Conflict with ISIS:
R. Fishel and A. Stein, "Lessons Learned from the Air War against the Islamic State", *War on the Rocks*, 23 February 2018.

[59] For examples of key air power scholars and central texts, see:
G. Douhet, *The Command of the Air*, trans. D. Ferrari (Alabama: Air University Press, 1921).
H. Trenchard, "The Effect of the Rise of Air Power on War", ed. Air Ministry Directorate of Staff Duties (London: UK, 1946).
W. Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military* (Alabama: University of Alabama Press, 1925).
A. Seversky, *Victory through Air Power* (New York: Simon and Schuster, 1942).
Pape, *Bombing to Win: Air Power and Coercion in War*
J.A. Warden, "Strategy and Airpower", *Air and Space Power Journal* Spring (2011).

[60] Nye, "Public Diplomacy and Soft Power".
J. McClory, "The New Persuaders: An International Ranking of Soft Power", (Instiute for Government 2010).

[61] For Lowther's arguments, see:

Finally considering smart power, depth on this concept which was coined by Nye but popularised by Hillary Clinton is offered in a breadth of academic and official literature[62]. Though not directly relating to air power, its analysis combined with the previously mentioned literature on hard and soft power, positions sufficient evidence to underpin the arguments presented in the thesis[63].

Turning next to the depth on how power is translated to influence through the application of state objectives, and the importance air power plays in this achievement of strategic level intent, the founding literature is offered in the academic understanding of strategy. With a breadth of writing on the topic from scholars including Porter and Betts, a theoretical foundation is created[64]. Though other national frameworks are considered in the subsequent practical examination of the strategic value of air power, the UK's *protect, project* and *promote* objectives are adopted as ideal to structure the arguments[65].

A.B. Lowther, "Air Diplomacy: Protecting American National Interests", *Strategic Studies Quarterly,* 4, no. 3 (2010).
For supporting literature on Lowther's humanitarian element, see:
K. M. O'Connell, "'Uncle Wiggle Wings': Children, Chocolates and the Berlin Airlift", *Food and Foodways,* 25, no. 2 (2017).
H. Venhuizen, "Air Force C-17s Delivering Relief to Beirut Following Deadly Explosions'", *Military Times*2020.
D.F. Harrington, "The Berlin Blockade Revisited", *The International History Review,* 6, no. 1 (1984).
For supporting comment on Lowther's public engagement element, see:
BBC, "Red Arrows Touch Down in China on World Tour", https://www.bbc.co.uk/news/uk-england-lincolnshire-37739750.
For supporting literature on Lowther's capacity building element, see:
C. Atkinson, *Military Soft Power: Public Diplomacy through Military Educational Exchanges* (Lanham: Rowman & Littlefield, 2014).

[62] For Nye's coining of smart power, see:
J.S. Nye, "Combining Hard and Soft Power", *Foreign Affairs,* 68, no. 4 (2009).
For Clinton's use of smart power, see:
H. Clinton, "Transcript of Clinton's Confirmation Hearing to the Senate Foreign Relations Committee", *NPR,* (2009).

[63] For examples of developing thinking in smart power which support the thesis alignment of it with air power, see:
N.C. Crawford, "Just War Theory and the Us Counter Terror War", *Perspectives on Politics,* 1, no. 1 (2003).
Augustine, *The City of Gods: Against the Pagans* (Cambridge: Cambridge University Press, 413-426 BC).
K.A. Annan, "Secretary-General's Annual Report to the Un General Assembly ", ed. UN General Assembly (New York United Nations 2005).
K.A. Annan, "We the Peoples: The Role of the United Nations in the 21st Century ", (New York: United Nations, 2000).
G. Evans and M. Sahnoun, *International Commission on Intervention and State Sovereignty (Iciss), the Responsibility to Protect* (Ottawa: International Development Research Centre, 2001).
UN, "2005 World Summit Outcome Document ", (2005).

[64] P. Porter, *The Global Village Myth: Distance, War and the Limits of Power* (Georgetown: Georgetown University Press, 2015).
R.K. Betts, "Is Strategy an Illusion?", *International Security,* 25, no. 2 (2000).

[65] Examples of National Security Strategies considered include:
US, "National Security Strategy of the United States of America", ed. President of the United States (2017).
UK, "Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy", ed. HM Government (2021).
Australia, "Strong and Secure: A Strategy for Australia's National Security", ed. Department of the Prime Minister and Cabinet (Australia Australia 2013).
Republique-Française, "Defence and National Security Review: Strategic Review ", (France2017).

In the first, protecting national sovereignty, the body of evidence is considerable. Represented through a broad mix of academic, governmental, industry and media sources, the collective evidence proves how air power has become central to the modern protection of states. For example, in exploring the assurance of aerial sovereignty in the era of powered flight, books including Banner's *Who Owns the Sky* are combined with peer-reviewed journals such as Williams' *A Crisis in Aerial Sovereignty* and governmental publications from sources including the UK to the Paris Convention papers to deliver a clear argument that air power is a lynchpin of contemporary national sovereignty[66]. With this theme of a breadth of sources creating depth repeated across the *project* and *promote* objectives, a clear foundation of literature is delivered to offer a firm assessment that air power is at a strategic level vital to assuring the role and survival of states.

Though this conclusion is balanced by the thesis in its acknowledgment that states reliance on air power is not absolute, but dependant on the role the state plays and whether it faces an existential threat, the overarching theme and interlocking nature of two factors is clear. Firstly, air power for most states is a pivotal capability that if lost or compromised will have strategic impact. Secondly, though in parts literature must be reinterpreted from broader discussions and its utility to air power confirmed, there is a significant body of academic writing supported by governmental, industry and media sources which underpin the assertion and allow the research to be developed and delivered with rigour.

The Gap in Knowledge: A Missing 'Golden Thread'

Reflecting on the above summary of the literature that has been engaged with across a breadth of sources, it is evident that though analysis and reinterpretation is required there are no significant gaps in academic understanding in either the

[66] S. Banner, *Who Owns the Sky? The Struggle to Control Airspace from the Wright Brothers On* (Cambridge MA: Harvard University Press, 2008).
Williams, "A Crisis in Aerial Sovereignty? Considering the Implications of Event Military Violations of National Airspace".
ParisConvention, "Convention for the Regulation of Aerial Navigation", *The American Journal of International Law,* 17, no. 4 (1923).
UK, "Aviation Cyber Security Strategy: Moving Britain Ahead", ed. Department for Transport (2018).

operational or strategic level discussions of air power's cyber risk. What these resources therefore allow is the thesis to chart a clear argument as to why there is a credible cyber risk to air power at an operational level and how if air power were to be lost or compromised the strategic ramifications for states would be momentous. Employing this literature to develop and deliver the argument throughout, the extensive references quoted in the body of the thesis and listed in the bibliography confirm the extent and legitimacy of the evidence.

However, the research behind the thesis has identified a significant and key gap in knowledge. Notably, the evidence for the operational level causes of air power's cyber risk is clear. Though in parts not air power specific, but in all air power relevant, discussions across the vulnerabilities and threats confirm that hostile actors will in time exploit clear weaknesses. Equally, at a strategic level, arguments underpinned by air power theorists and developed through an understanding of governmental objectives show how the loss of air power would have immense consequences for most states. What has not been discussed, and where the clear and concerning gap in academic understanding exists, is the 'golden thread' which explains and charts the causal relationship between the operational causes and strategic consequences of air power's cyber risk.

Though to date some academic discussion has highlighted the localised impact, none has charted with clarity how operational cyber risk will have significant, and potentially immediate, impact on nation states. Further, though some literature does discuss the embryonic nature of the risk, none has made the clear and pressing argument that it will in time mature to a point at which it will change the pathway of the 21st century unless recognised by the academic community and understood, managed, and mitigated by practitioners.

It is this gap in the academic charting of the 'golden thread' and issuing of a clear warning that the thesis addresses. Developed through the case study-based Part 3 which culminates in three scenarios exploring how the risk may manifest, a clear call to action is offered. In this, the thesis does not claim to fill the identified gap in knowledge but does position itself as an intellectual springboard upon which the academic community can develop. If embraced, and the springboard used, the void in knowledge that exists between the operational and strategic levels could be filled and, in turn, the most severe consequences of air power's cyber risk actively managed so that it can be effectively mitigated.

Conclusion

This opening chapter of the thesis has framed the following discussions by offering an introduction to the digitisation of air power before providing an overarching review of the academic, governmental, industry and media literature that allows the arguments to be expressed. It further illuminated a distinct gap in knowledge which has until now failed to identify the 'golden thread' that exists between how these causes will lead to strategic level consequences. By doing so, the chapter finally confirmed that whilst the thesis will not in isolation fill this gap it does intend to act as an intellectual springboard to ensure the gap is recognised, action is taken, and the most cataclysmic consequences prevented.

With this justification of the research and its viability based on existing literature offered, the next two chapters of this opening part will introduce in turn the key term of cyber and the foundational IR concepts that ground the research. In doing so, the aim is to ensure that the thesis is accessible to, and will act as a catalyst for, both the academic and practitioner communities who must work in synergy if this gap in knowledge is to be filled and the strategic implications managed.

Chapter 2: Cyber - The Underlying Concept

Introduction

Building on the previous discussion of the gap in knowledge which this thesis illuminates, this chapter explores the term cyber. Initially identifying it as a pre-fixing shorthand to describe all digitally related concepts, it will be acknowledged as overtly simple and, in the view of some academics, moribund. However, in its nuance, it will be shown to have validity if offered depth via one of two definitional approaches: hardware and software centric or more holistic alternatives.

Exploring these, the discussion will acknowledge that any complete analysis of cyber must include the core focus of software and hardware. However, it will also be argued through the application of relevant models that other more holistic elements including people and infrastructure must also be considered.

Building on this assertion, the discussion will next explore how the digitisation of air power across all relevant areas could have significant impact. This digitisation will in turn, it will be concluded, place air power at an increased risk of compromise. Notwithstanding this, it will finally be asserted that before any meaningful research can be conducted, especially at the level of nation states, a further discussion to introduce, understand and choose a relevant IR paradigm is essential. It is this requirement that Chapter 3 will address.

Defining Cyber

The shorthand of terminology allows a word to be coupled with a complex idea so that knowledge may be shared more efficiently. Reflecting on this, Lydiate notes that in all discipline's terminology, even when used with the best of intentions, can be misunderstood[67]. Before exploring the concept of air power's cyber risk in depth, one must therefore introduce and define the underpinning

[67] D. Lydiate, "Swimming with Our Eyes Open", *ITNOW,* (2020).

term of cyber and, through this, identify an accessible framework to guide the research.

With technology actively shaping our lives, it might be assumed that even without expert knowledge most of us will hold a basic understanding of cyber[68]. However, as illustrated by Foster-Wallace's parable, few people stop to reflect on what they routinely interact with:

> There are two young fish swimming along and they happen to meet an older fish swimming the other way, who nods at them and says "Morning, boys. How's the water?"
>
> The two young fish swim on for a bit, and then eventually one of them looks over at the other and goes "what the hell is water?"[69]

Clarifying his point, Foster-Wallace explains that the most important realities are the hardest to see[70]. Whilst he refers to education, Macak views the parable as having value in technology which though 'invisible to the naked eye, has profound impact'[71]. This makes it to most of us what water is to fish; something we seldom consider.

Failing to recognise this technological 'water' in which we swim, most of us also fail to reflect on the concepts that are used to discuss it. Key to these is cyber. A term traced to Weiner's 1948 coining of cybernetics, a reuse of the Ancient Greek *kybernētēs*, its reinventions have been numerous[72]. Initially driven by the arts through works such as Ussing's *Cyberspace* and Gibson's novel *Neuromancer,*

[68] Discussing the impact of technology on our daily lives, Bridle comments that it is no longer 'merely augmenting our lives…[but] shaping and directing them'.
J. Bridle, "Rise of the Machines: Has Technology Evolved Beyond Our Control?", *The Guardian*, 15 June 2018.

[69] This parable was presented by Foster-Wallace in a commencement speech to Kenyon College, Ohio, in 2005.
D. Foster-Wallace, "This Is Water", *Commencement Speech to Kenyon College, Ohio,* (2005).

[70] Ibid.

[71] K. Macak, "This Is Cyber: 1+3 Challenges for the Application of International Law in Cyberspace", *Working Paper Series, Exeter Centre for International Law* (2019): 1.

[72] For Weiner, see:
N. Weiner, *Cybernetics: Control and Communication in the Animal and the Machine* (Cambridge, MA: MIT Press, 1948).
For the reuse of the ancient Greek term, see:
S. Levinson, *Mathematical Models for Speech Technology* (Illinois: Wiley, 2005), 200.

this continued until technologists finally re-appropriated the term[73]. Now considered an adjective relating to the culture of computers, its value remains, as Weiner initiated, in its use as a prefix[74].

Becoming entrenched in modern lexicon, this prefixing is frequently used to describe every digital related concept from the consumer driven 'cyber Monday' to the security focused 'cyber hygiene'[75]. The result of this broad and often unreflective use of 'cyber' is that most people have, even those engaged in digital industries or digitally focused research, become the 'young fish'. When such 'young fish' manifest in the context of digital means as a route to undermine the military lever of power, such a lack of clarity creates a much greater level of concern than when 'cyber' is used to describe a more benign topic such as a cut-price online shopping event.

Engaging in this discussion with specific reference to security, Futter argued in 2018 that the solution is to retire the buzzword of cyber[76]. Presented over five interlocking arguments, he asserts that from its introduction through articles including Aquilla and Ronfeldt's seminal 1993 'Cyber War is Coming!'[77], to its 'disjointed evolution' and contemporary use as a catchall, cyber has become a homogenous one-size-fits all concept. Universally adopted despite this lack of clarity, scholars and officials alike have in Futter's estimation been confused by the ill-defined term to the point at which its complexities are routinely cloaked. Bringing his argument together, Futter concludes that the only viable option is for the 'all-conquering 'cyber' moniker' to be replaced in both academic and policy discussions with more precise technical language[78]. If this were to be achieved,

[73] Ussing explored human perceptions of technology through a series of art works in the 1960s and 70s. For depth, see:
Lillemose A. Lillemose and Krygerm M., "The (Re)Invention of Cyberspace", *The Nordic Art Review,* (2015)., A. and Krygerm M. 'The (Re)Invention of Cyberspace, *The Nordic Art Review*, 24 August (2015).
For Gibson, see:
W. Gibson, *Neuromancer* (New York: Ace, 1984).

[74] Oxford-Dictionary, "Definition of Cyber " in *Oxford Dictionary* (Oxford Oxford University Press, 2015).

[75] For a discussion of 'Cyber Monday', see:
O. Tambini, "Black Friday Vs Cyber Monday: What's the Difference?", *Techradar*, 14 November 2019.
For a discussion of 'Cyber Hygiene', see:
UK, "The Uk Cyber Security Strategy Protecting and Promoting the Uk in a Digital World", ed. Cabinet Office (HM Government 2011), 31.

[76] A. Futter, "Cyber Semantics: Why We Should Retire the Latest Buzzword in Security Studies", *Journal of Cyber Policy,* 3, no. 2 (2018).

[77] Arquilla and Ronfeldt, "Cyberwar Is Coming!".
Weiner, *Cybernetics: Control and Communication in the Animal and the Machine*

[78] Futter, "Cyber Semantics: Why We Should Retire the Latest Buzzword in Security Studies", 208.

he asserts that 'linguistic clarity, precision and acceptance' can emerge allowing those engaged in security to properly 'understand, conceptualise and mitigate the most pressing…challenges of the current information age'[79].

From a scholarly perspective, Futter's arguments cannot be faulted with the narrative illustrating a term that through its wholesale use has become meaningless. This argument was pre-empted by Walt who as early as 2010 identified the problematic nature of lumping the whole topic of technology together under a 'single banner' of 'cyber'. It could therefore be concluded that this thesis is itself adding to the issues by using the term in a single statement to address the expansive issue of air power's technologically founded risk.

Where Futter's analysis can be critiqued, however, is that whilst misunderstanding surrounds the term cyber, and many continue to use it loosely and inaccurately, it has become so ingrained in modern lexicon that to remove it altogether is virtually impossible. An argument articulated by Dickson with specific reference to Government and Military organisations, he concludes that not only are these groups 'comfortable with the term…[but] there are many instances where the term is so baked into government code, signage, and doctrine that a simple name change would cost taxpayers billions'[80]. Therefore, a pragmatic position is to acknowledge Futter's argument and the issues it raises, but shift focus from removing the term cyber from all discussion to actively defining not just the word but its underlying elements. If achieved with a supporting lexicon to unpick its complexities, we might reverse the pervasive lack of clarity and achieve the level of focused discussion required to properly 'understand, conceptualise and mitigate' the pressing digital security challenges[81].

To move towards achieving this intent, it is necessary to first dissipate the smokescreen that cyber's ill-defined use has created. In doing so with a pragmatic eye, one finds that attempts to define cyber and create an underpinning lexicon are numerous. When analysed these attempts can be broken into two

[79] Ibid., 216.
[80] J. Dickson, "We Need a New Word for Cyber", *Dark Reading* 23 November 2015.
[81] Futter, "Cyber Semantics: Why We Should Retire the Latest Buzzword in Security Studies", 216.

broad schools of thought: system and network centric definitions and holistic definitions[82].

Endorsing the first, system and network centric definitions, Nye states that cyber should be considered 'a prefix standing for electronic and computer related activities'[83]. Supported by Kuehl who defines cyber as framed by our use of electronics, these academic approaches are representative of most governmental thinking[84]. Given this, one might assume that there is broad agreement that cyber should be limited to describing the hardware and software that constitutes systems and networks.

This interpretation has however been disputed by holistic definitions. Futter himself, for example, suggests that the 'cyber challenge' should be thought of as not just comprising software and hardware but also the people who engage with them[85]. Given depth by Singer and Friedman who acknowledge that whilst cyber is an information environment it is not purely virtual, we are presented with a reality in which cyber must be defined as much by the people which interact with it as it is by its physical or digital aspects[86].

It is therefore acknowledged that any complete conceptualisation of the term cyber must include the core elements of software and hardware in both their digital and physical manifestations. However, to other commentators this division alone is not comprehensive enough. Rather, it has been argued that a definition must go further and consider the human element in terms of not only human-

[82] Discussing the definitions of cyber, Nye comments that any definitive understanding is made challenging by the fact that there are literally dozens of versions to choose from. This is underlined by Futter who comments that because debates in this area remain 'in the eye of the beholder' the identification of a single definition all can agree upon is virtually impossible.

Nye, *Cyber Power*, 3.

A. Futter, "Hacking the Bomb: Nuclear Weapons in the Cyber Age", in *ISA Annual Conference* (New Orleans2015), 4.

[83] Nye, *Cyber Power*, 3.

[84] For Kuehl's full definition of cyber, see:

Kuehl, "From Cyberspace to Cyber Power: Defining the Problem," 4.

For an example of Governmental thinking on cyber, see:

US, "The National Strategy to Secure Cyberspace", ed. White House (2003), 1.

"National Military Strategy for Cyberspace Operations", ed. Department of Defence (2003), 3.

[85] Futter, "Hacking the Bomb: Nuclear Weapons in the Cyber Age", 4.

[86] P.W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford Oxford University Press, 2014), 14.

machine interaction but also a cognitive space in which people interact with, and exist in, the digital world.

Modelling Cyber

Having established this holistic definition of cyber as the foundational understanding, it is next necessary to identify an aligned framework upon which the thesis can be developed. One academic model which provides such a basic framework is cyber littorals.

Adopting an oceanographic term meaning the area of water near the shore and the area of shore near the water[87], cyber littorals are defined by Withers as the point at which 'the hardware and software of cyberspace come into contact with the physical and cognitive world'[88]. Though explaining the edges of cyber, and therefore where the interaction with the cyber environment occurs, Withers acknowledges that if all elements were included in the 'cyber littoral zone' the grouping would become so large that the model, and therefore its characterisation of cyber, would no longer be of value[89].

A solution to this is again offered by Futter who categorises cyber activities into three areas: physical, logical, and human [90]. Whilst elegant, a more comprehensive model following similar logic is provided by UK military doctrine. Specifically, the *Cyber Primer's* 'Layers of Cyberspace' model describes cyberspace as a complex, dynamic and 'all-encompassing operating environment'[91]. Further examining the environment, the model delivers the context necessary for this research by subdividing cyber into three layers: the people, real, and information layers[92].

[87] J. A. Peters and D. M. Lodge, "Littoral Zone," in *Encyclopaedia of Waters* ed. G. E. Likens (New York: Elsevier, 2009).
[88] Withers, "What Is the Utility of the Fifth Domain?", 133.
[89] Withers includes the following elements as being among those which should be considered to be in the 'cyber littoral zone': 'physical infrastructure, cabling and electrical power; the electromagnetic spectrum that data traverses; electro-mechanical processes under computer control; and the senses and cognition of computer users'.
Ibid.
[90] Futter, "Hacking the Bomb: Nuclear Weapons in the Cyber Age", 4.
[91] UK, "Cyber Primer", ed. Ministry of Defence (2016), 5.
[92] Ibid.

Transposing this model into the thesis' cross-disciplinary examination of air power's cyber risk we are presented with a meaningful multi-layered definition of cyber. Firstly, air power like all digitally enhanced industries is in all its forms developed, delivered, maintained, and operated by people. Though contradicted in some respects using technology to achieve automation and replace the human, people remain key to its processes. Therefore, even in a technologically driven discussion of air power's cyber risk, the people layer must loom large.

Secondly, air power is by its nature manifested through tangible assets ranging from ground-based infrastructures including fuels and Air Traffic Control (ATC) to physical air platforms. Understanding how the digital element of cyber interacts with, and may affect, these physical realities is therefore essential.

Finally, and possibly most intuitively, the information layer within which air power processes, stores, and outputs its digital information forms the core of advanced air power. Because of this, it must also be closely examined within any exploration of air power's cyber risk.

Reflecting on this conceptualisation of cyber, a perspective is unveiled which has been grown from the kernel of Weiner's 1948 cybernetics but emerges as a practical understanding of a complex environment[93]. Adopted as a framework for the subsequent exploration of air power's cyber risk, this holistic definition identifies cyber as a term encompassing a multi-layered environment. At its core, a logical layer of digital information is stored and processed on systems and networks. These are, however, intrinsically entwined in its literals with the real layer of physical infrastructure and a people layer of human interaction. Though it is acknowledged that an underpinning lexicon is required to allow the logical, physical and people layers to be discussed with clarity, it is asserted that as we move towards this position the umbrella term of cyber is no longer moribund as Futter suggests. Rather, its contextualised use enriches our understanding of a complex digital environment. Adopting this foundation, the thesis will in the

[93] Weiner, *Cybernetics: Control and Communication in the Animal and the Machine*

following chapters apply this definitional understanding of cyber to explore in depth the causes and consequences of air power's cyber risk.

Conclusion

Identifying how the use of cyber as shorthand to simplify a complex issue has led to a lack of clarity in technological discussions, this chapter sought to establish a definitional baseline for the thesis. Outlining how the word developed and emerged in modern lexicon as a prefix describing all digitally related concepts, Futter's arguments on the need to remove the term cyber from discussion were explored. Though the validity of this contention was recognised, it was ultimately assessed that given its 'baked in' status within modern lexicon a more pragmatic approach was to seek a clear definition of the term.

Having explored the options to achieve this, it was acknowledged that any complete analysis of cyber must include the core elements of software and hardware. However, in looking wider and considering relevant models, the chapter also concluded that to fully understand the topic a holistic approach must be adopted. This should incorporate other key elements of the wider cyber domain including, in its littorals, people and infrastructure.

Though offering a firm foundation to understand cyber, there is a requirement to next offer an understanding of IR. Key to appreciating the theoretical blocks on which this thesis is built, this will offer the final underpinning element before the examination of the causes of air power's cyber risk can be delivered in Part 2.

Chapter 3: International Relations (IR) - The Analytical Lense

Introduction

To ensure the thesis is accessible to both IR scholars and practitioners, this chapter builds on the previous introduction to cyber by offering a foundational understanding of IR and clarity on the theoretical underpinnings of the research. Notably, the individual IR paradigms will be considered before an argument is made for the adoption of a pluralistic realist-constructivist paradigm. In doing so, the theoretical basis for this thesis will be established.

Demystifying the IR Paradigms

Like all disciplines, IR is cloaked in terminology which, though familiar to IR scholars, is alien to outsiders. To demystify this, it is necessary to introduce the discipline.

Though founded on thousands of years of political and philosophical thought, modern IR and its lexicon are linked to a select group of mid-20th century scholars[94]. Including influential thinkers such as Carr and Morgenthau[95], this cadre defined the broad analytical frameworks that guide the discipline. Ultimately delivering theoretical tool sets that allow scholars to identify and understand patterns, IR is now recognised as the means through which global political events are interpreted and predicted[96].

Developed over the interceding century, competing assertions have led to the emergence of distinct analytical options for IR research. Variously referred to as 'perspectives', 'discourses' or 'schools of thought', exploring these can be

[94] For example, the Athenian philosopher Thucydides who lived in c.400-460 BC is often quoted as being the founding father of the realist paradigm. For further discussion on the long history of realism in IR thinking, see:
S. Forde, "Varieties of Realism: Thucydides and Machiavelli", *The Journal of Politics,* 54, no. 2 (1992): 3762.

[95] For example, seminal texts which are often quoted as being influential in the development of IR include Carr's 1929 book *Twenty Years Crisis* and Morgenthau's 1963 book *Politics Among Nations*.
E.H. Carr, *Twenty Years Crisis: 1919-1939* (London: Palgrave Macmillan, 1939).
H.J. Morgenthau, *Politics among Nations: The Struggle for Power and Peace* (New York: Knopf, 1948).

[96] For depth on the development of the modern IR discipline, see:
Burchill et al., *Theories of International Relations*, 1.

confusing. For this thesis these IR frameworks will therefore be referred to as 'paradigms', a term which Keene succinctly defines as describing the work of a community of scholars who can be distinguished as agreeing on common themes of the major questions[97]. Though variations in these paradigms exist, those commonly associated with contemporary IR are realism, liberalism, and constructivism. To confirm which of these offers the most appropriate baseline for this thesis, each will be considered in turn.

The Realist Narrative: Explaining Survival but Leaving Questions Unanswered

An intuitive starting point is realism which asserts that though a peaceful world may be desirable, humanity is by nature egotistic. As a result, there is no escape from the harsh truths of security, competition, and war[98]. When combined with the assertion that there is no legitimate form of international governance, a 'conflict-based paradigm' is created in which states are the key actors and power and security the main issues[99].

A dominant theme in IR, its providence can be traced from Thucydides, through Machiavelli*,* to Hobbes[100]. Forming the basis for contemporary realism, the

[97] E. Keenes, "Paradigms of International Relations: Bringing Politics Back In", *International Journal of Advances in Security,* 44, no. 1 (1989): 42.

[98] Discussing the realist paradigm, Hoffmann comments that realism is 'probably the most distinguished school of thought in the history of international relations'. However, other scholars have also labelled realism the most pessimistic. This direction of argument, alongside a summary of the foundations of realist thinking, are notably made by Mearsheimer in his book *The Tragedy of Great Power Politics.*

S. Hoffmann, *The Political Ethics of International Relations* (New York: Carnegie Council on Ethics and International Affairs, 1988), 6.

J.J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton Publishing Company, 2001), 97.

[99] W.J. Korab-Karpowicz, *Political Realism in International Relations - Stanford Encyclopaedia of Philosophy* (2010).

[100] For depth on Thucydides and his thinking, see:

J.S. Rusten, *Thucydides* (Oxford: Oxford University Press, 2009).

J. Marcus, "Could an Ancient Greek Have Predicted the Us-China Conflict?", *BBC News Online*, 25 March 2019.

G. Allison, "The Thucydides Trap: Are the Us and China Headed for War?", *The Atlantic*, 24 September 2015.

B. Zhang, "The Perils of Hubris? A Tragic Reading of 'Thucydides Trap' and China-Us Relations", *Journal of Chinese Political Science,* 2 (2019).

For Machiavelli's seminal realist test, see:

N. Machiavelli, *The Prince* (London: Penguin, 1513).

For the assertion that Machiavelli is one of the key fathers of realist thinking, see:

J. Leung, "Machiavelli and International Relations Theory", *Glendon Journal of International Studies,* 1 (2000): 1.

Korab-Karpowicz, *Political Realism in International Relations - Stanford Encyclopaedia of Philosophy*.

For Hobbes seminal realist text, see:

T. Hobbes, *Leviathan* (London: Penguin, 1651).

For discussions on Hobbes realist thinking, see:

H. Bull, "Hobbes and the International Anarchy", *Social Research* (1981): 718.

fundamental teachings which emerge are a characterisation of international politics as existing in anarchy, with states struggling for power and war being inevitable. Driven by a fundamental assumption that there is no right and wrong (only competing concepts of right), and no meaningful society beyond the state, a realist assertion is ingrained that states and their desire to achieve and maintain power are central to all discourse.

Speaking directly to the military lever of national power, these roots offer an intuitive foundation to the thesis' focus on air power. This is because if the world were not anarchic in the realist sense, military force would not be a central pillar of national power[101]. As it is, the premises of realism must not only be assumed correct but must also be the most logical paradigm on which to base this thesis.

This assertion on the natural alignment to realism is further supported by contemporary realist thinkers. Whether considering Carr's classical realist establishment of a 'hard-headed' view attuned to the true dynamics of power, or Waltz's neorealist argument that contends the structure of the international system forces states to seek power, the fundamental realist focus on anarchy and the desire to survive remains[102]. Striking a chord with the most basic of human instincts, the paradigm articulates why states are driven to create cutting-edge technologies to assure their survival. Further, and in the context of this

A.P. Martinich, *Hobbes* (London: Routledge, 2005), 6.
A.N. Yurdusev, "Thomas Hobbes and International Relations: From Realism to Rationalism", *Australian Journal of International Affairs,* 60, no. 2 (2006): 305.
J. Vincent, "The Hobbesian Tradition in Twentieth Century International Thought", *Journal of International Studies,* 10, no. 2 (1981): 93.

[101] This 'central pillar' claim is supported by Mearsheimer who comments that though states employ all the instruments of power to achieve national objectives, and these instruments include economic and diplomatic levers, it is the military lever which routinely comes to the fore when others fail.
Mearsheimer, *Structural Realism' in International Relations Theories: Discipline and Diversity* 72.

[102] For Carr's seminal realist work, see:
Carr, *Twenty Years Crisis: 1919-1939*.
For a discussion of Carr's works which are described as offering 'a brilliant restatement of Hobbesian themes' that would inform the development of all subsequent contemporary realist thinkers, see:
M. Wright, "Western Values in International Relations," in *Diplomatic Investigations: Essays in the Theory of International Politics*, ed. H. Butterfield and M. Wight (London: Allen and Unwin, 1966), 144.
For Waltz realist writings, see:
Waltz, *Theory of International Politics*
K.N. Waltz, "The Origins of War in Neorealism Theory", *Journal of Interdisciplinary History,* 18, no. 4 (1988): 618.
For a discussion of Waltz realist writings, see:
Forde, "Varieties of Realism: Thucydides and Machiavelli", 372.

thesis, it also explains why there is a necessity to secure these cutting-edge technologies as any failure to do so would undermine a state's ability to survive in an anarchial world.

Though this logic delivers a clear call for the thesis to be framed in the realist paradigm, it is noted that realism fails to address the complexities of human society. Specifically, in focusing on the anarchic nature of the world and the desire to survive, realism does not explain why at times mankind and the states it has created act with apparent motivations other than self-preservation. With advanced air power entwined with this tendency through its employment to further the strategic intent of states in ways that are not always tethered to survival, it would, despite the previous argument, be unintuitive to base this thesis purely within a realist paradigm.

The Liberalist Narrative: Attractive but Undermined by Reality

To address this concern and seek a richer foundation on which to frame the research, the next paradigm to consider is liberalism. Built on the ideal that people must be treated ethically, liberalism is encapsulated in three principles: negative freedom, or the freedom from arbitrary authority, positive freedom, or the right to protect and promote freedom, and democratic participation, or the right to have the means to guarantee the existence of positive and negative freedoms[103].

In terms of governance, these principles are rooted in the thinking of early philosophers including Locke. Describing a world in which a social contract exists, he argued that people will through democratic participation transfer some of their natural rights to the government in exchange for those rights being preserved[104]. Contextualised in the contemporary international system, liberal IR scholars would conclude that all states will in acting to uphold this social contract share

[103] M.W. Doyle, "Kant, Liberal Legacies and Foreign Affairs", *Philosophy and Public Affairs,* 12, no. 3 (1983): 206.

[104] For an examination of Locke's seminal work, *Second Treatise of Government,* and a discussion of his justification for war see:

J.A. Simmons, *Locke, Consent and the Limits of Society* (Princetown Princetown University Press, 1993), 13.

A. Tuckness, "Lockes Political Philosophy," in *Stanford Encyclopaedia of Philosophy* ed. E.N. Zalta (Stanford Stanford University Press, 2005).

common interests in peace and prosperity to assure their people's rights whilst concurrently respecting the rights of people in other states[105].

Though an attractive counterbalance to realism, liberalism fails to account for the dominance of the military lever of power and, within this, the existence of advanced air power. Though Locke himself acknowledges that conflict may be necessary where the social contract has been broken, he does not consider war to be within the natural condition of man. However, as war and offensive military capabilities including air power undeniably exist, and the loss of these capabilities is proposed by this thesis as likely to unbalance states, such liberal arguments are shown to be idealistic, but not realistic and therefore unsuitable for this thesis.

Constructivism: The Missing Piece

Reflecting on this rejection of liberalism, and the judgement that realism is in isolation too narrow, it is necessary to look further. To do so, the final paradigm to consider is constructivism.

Challenging established thinking, constructivism is driven by the overarching theme that international politics is 'historically contingent' rather than naturally occurring. Delivering an ability to explain events which realism and liberalism failed to predict, constructivism has become an increasingly popular third option for IR scholars[106]. However, with critics claiming it to be an 'empty vessel' which fails to prescribe a social ontology, the paradigm remains contentious[107].

First emerging as idealism in the interwar years as a reaction to the horrors of the First World War built on the philosophies of Grotius, Kant, and Hegel, the approach sought to achieve a socially constructed harmonious world that would challenge realism and the perceived inevitability of war[108]. Though leading to the

[105] For a development of these basic premises of liberalism in international affairs, see:
Doyle, "Kant, Liberal Legacies and Foreign Affairs", 213.

[106] P.T. Jackson and D.H. Nexon, "Whence Casual Mechanisms? A Comment on Legro", *Dialogue IO,* 1, no. 1 (2002): 82.

[107] For an expansion of these criticisms of constructivism, see:
T. Flockhart, "Constructivism and Foreign Policy," in *Foreign Policy*, ed. S. Smith (Oxford Oxford University Press, 2008), 81.

[108] A. Wendt, *Social Theory of International Politics* (Cambridge Cambridge University Press, 1999), 3.

League of Nations, its dominance was both brief and criticised as underestimating power and overestimating law, morality, and public opinion[109].

Despite its short tenure, idealisms base concepts would reemerge in the 1950s as the English School[110]. Honed over the next three decades it would focus on one central question which came to underpin contemporary constructivism: how can the co-operative aspect of international relations be reconciled with the realist conception of anarchy and conflict in the international system?[111]

Catalysed by realism and liberalism failing to predict the end of the Cold War, constructivism, a term coined by Onuf[112], would emerge from this central question in the early 1990s to explain why ideas and identities drive the actions of states[113]. A position succinctly summarised by Wendt, he defined the paradigm as consisting of three principles. Firstly, all people, and therefore states, act towards all objects, including other actors, based on the meanings that they have for them. A state will therefore act differently towards an enemy than a friend because of

[109] This overview of idealism is derived from:
P. Wilson, "Idealism in International Relations," in *Encyclopaedia of Power*, ed. K. Dowding (Thousand Oaks: Sage, 2011), 332.
L.M. Ashworth, "Where Are the Idealists in Interwar International Relations?", *Review of International Studies,* 32 (2006).
For specific comment on the League of Nations, see:
C. Townshead, "The League of Nations and the United Nations", *BBC History* 2017.
For further detail on Carr's arguments against idealism, see:
Carr, *Twenty Years Crisis: 1919-1939*.
For additional analysis on arguments against idealism, see:
D. Long and P. Wilson, *Thinkers of the Twenty Years' Crisis: Inter-War Idealism Reassessed* (Oxford Oxford University Press, 1995), 1.

[110] The English School was largely derived from the thinking emanating from the British Committee of Theory of International Politics. For depth, see:
T. Dunne, "The English School," in *The Oxford Handbook of Political Science* ed. R.E. Goodin (Oxford: Oxford University Press, 2011), 3.

[111] Key works which epitomise the development of the English School are commonly considered to include:
H. Bull, *The Anarchical Society: A Study of Order in World Politics* (London: MacMillan Press, 1977).
M. Wight, *System of States* (Leicester Leicester University Press, 1977).
For depth on the English School's development, see:
B. Buzan, "The English School: An Underexploited Resource in Ir", *Review of International Studies,* 27, no. 3 (2001).
O. Waever, "Four Meanings of International Society: A Trans-Atlantic Dialogue," in *International Society and the Development of International Relations Theory* ed. B.A. Roberson (London: Pinter, 1998).
For discussion on the similarities between contemporary constructivism, see:
C. Reus-Smit, "Constructivism and the English School," in *Theorising International Society* ed. C. Navari (London: Palgrave Macmillan, 2009), 58.
For depth and comparative analysis, see:
R. Little, "Neorealism and the English School: A Methodological, Ontological and Theoretical Reassessment", *European Journal of International Relations,* 1, no. 1 (1995): 10.

[111] This second phase of the English School from 1966 is most notably associated with Bull's *The Anarchical Society* and Wight's *System of States*.
Bull, *The Anarchical Society: A Study of Order in World Politics*
Wight, *System of States*.

[112] N.G. Onuf, *World of Our Making* (South Carolina: University of South Carolina Press, 1989).

[113] S.M. Walt, "International Relations: One World, Many Theories", *Foreign Policy,* 110 (1998): 41.

the social context of their relationship. Secondly, to guide the social interactions of the first principle, states will assume stable and distinct identities and roles through which a definable structure will be created. Finally, international organisations will act as a stabilising factor for states as they pursue the interests associated with their identities[114].

Addressing realisms failure to consider the complexities of human society, Wendt's principles deliver this thesis a toolset to examine air power's cyber risk. This assertion is given further depth by including a sub-set of constructivism, role theory.

Encased in Wendt's second principle, role theory began life as a theatrical metaphor[115]. Reflecting the fact that actors are constrained because of the 'parts' written for them, sociologists theorised that the behaviours of people could also be predicted by the 'roles' they play in society[116]. Translated into mainstream IR in the 1960s and 70s[117], theorists including Holsti adopted role theory to not only define the roles of states but also understand and predict their actions[118]. Though critics warn that any single role definition presents too crude a characterisation[119], by including other sub-distinctions such as the line between roles and status

[114] Wednt's three principles of constructivism are set out in:
Wendt, "Anarchy Is What States Make of It: The Social Construct of Power Politics", 399.
Building on Wendt's writing, Checkel follows the logic in his two assumptions on constructivism. For these, see:
J.T. Checkel, "The Constructivist Turn in International Relations Theory", *World Politics,* 50, no. 2 (1998): 326.

[115] S. Harnisch, C. Frank, and H.W. Mauli, *Role Theory in International Relations: Approaches and Analyses* (London: Routledge, 2011), 1.

[116] B.J. Biddle, "Recent Developments in Role Theory", *Annual Review of Sociology*, no. 12 (1986): 68.

[117] An early example of a form of role theory being employed in an IR context can be found in the works of German diplomat von Kuhlmann.
R. VonKuhlmann, "The Permanent Bases of German Foreign Policy", *Foreign Affairs,* 9, no. 2 (1931): 179.
Role theory would again resurface in the 1960s and 70s. For example, see:
H. Sprout, Sprout, M. , "Environmental Factors in the Study of International Politics", *The Journal of Conflict Resolution,* 1, no. 4 (1957): 318.
K. Holsti, "National Role Conceptions in the Study of Foreign Policy", *International Studies Quarterly,* 14 (1970): 233.

[118] Holsti's initial definitions of sates roles included 'non-aligned', 'bloc leaders', 'balancers' and 'satellites'. For depth, see:
"National Role Conceptions in the Study of Foreign Policy".
Wish cites the work of Sarbin and Allen as key influencers in the application of social psychology role theory to the international context. For detail, see:
N.B. Wish, "Foreign Policy Makers and Their National Role Conceptions", ibid.24, no. 4 (1989): 534.
For further discussions on how role theory was developed in IR, see:
T.R. Sarbin and V.L. Allen, "Role Theory," in *The Handbook of Social Psychology*, ed. Lindzey. G. and E. Aronson (Reading MA: Addison-Wesley, 1968), 522.
Harnisch, Frank, and Mauli, *Role Theory in International Relations: Approaches and Analyses* 7.

[119] Holsti, "National Role Conceptions in the Study of Foreign Policy", 234.

contextualised depth is offered and value to understanding states actions on the international stage is achieved[120].

Transposed to this thesis, the advantages of constructivism are clear. With realism explaining the underlying motivations of states, constructivism contextualises the way in which motivations manifest. Offering a valuable tool set, it presents an opportunity for the research to explore how the causes of air power's cyber risk have developed and, through case studies, consider in depth explanations for its consequences. However, as noted, to achieve this constructivism must be supported by the underlying truths of realism.

A Pragmatic Solution: Pluralism and the Realist-Constructivist Paradigm

Reflecting on the mutual advantages of realism and constructivism, the thesis' exploration of the strategic consequences of air power's cyber risk is logically led to a pluralistic paradigm which allows 'the tensions and contradictions of the world' to be accounted for[121]. Supported by Barkin who suggests that as all IR paradigms display natural affinities, it is reasonable, he argues, to discount pre-defined lines which only exist because of the pedagogy of IR[122].

Not necessarily contentious, the choice of such an 'inter-paradigm' path has been a consistent refrain within IR. Illustrated by prominent scholars including Waltz in neorealism, Keohane in neoliberalism and Wendt in constructivism, it can be

[120] It is acknowledged that this discussion of roles in the context of constructivist thinking has focused on role theory and not discussed the associated concept of status. Easily confused or misused, the two, as Le Prestre notes, are both distinct but, at the same time, maintain a symbiotic relationship. This distinction is explained by Blagden as status being concerned with the relative standing and recognition of a state within the socially constructed international society and role focusing more on the performance of a state. Therefore, when discussing a state's role or performance this thesis is also in an associated context discussing the status which is derived from playing the specific role.

P.G. LePrestre, *Role Quests in the Post-Cold War Era* (London: McGill-Queen's University Press, 1997).

D. Blagden, "Two Visions of Greatness: Roleplay and Realpolitik in Uk Strategic Posture", *Foreign Policy Analysis,* 15 (2019): 474.

This conclusion is supported by Le Prestre who concludes that understanding a state's self-accepted role definition can enrich IR research and help to explain a state's actions.

LePrestre, *Role Quests in the Post-Cold War Era* 5.

[121] R.H. Jackson, "Pluralism in International Relations", *Review of International Studies,* 18, no. 3 (1992): 281.

[122] Barkin's arguments are supported by Schmidt who contends that in 'an increasingly complex world…[which is] faced with a myriad of issues ranging from global climate change to the continuing risk of nuclear Armageddon…we need a variety of different theories to help us make sense of the world'.

S.J. Barkin, *Realist Constructivism* (Cambridge Cambridge University Press, 2012), 162.

B. Schmidt, "International Relations Theory: Hegemony or Pluralism?", *International Relations Theory,* 36, no. 2 (2007): 106.

concluded that pluralism has been proven to be not only possible but valuable[123]. Acknowledging this, the key question to ask is whether the above suggestion of combining realism and constructivism is the most suitable pluralistic solution for this thesis?

An option explored by Barkin, it is suggested that if constructivism had not been routinely presented as a challenger to realism theorists would have more readily acknowledge that the two are mutually supportive[124]. Driven by the core pluralist argument that when the complexities of reality are brought into the discussion no single paradigm provides a suitable explanation, collective analysis of the two offers synergistic advantages[125]. Supported by Lebow who comments that the two paradigms offer 'separate but interlocking pieces' that solve larger IR puzzles[126], he concludes that to achieve a comprehensive understanding one must adopt 'a synergistic, cross-paradigm approach' that envelops both realism and constructivism[127].

With other academics identifying further synergies across the concepts of roles, power politics, anarchy, and self-help behaviours, this pluralistic realist-constructivist approach is shown to be valid[128]. Having in truth already been embraced by a plethora of other scholars, it can be concluded that this thesis'

[123] This list of IR scholars with pluralistic tendencies is provided by Bennett who identifies the following texts as touchstones in the relevant sub-discipline's discussions:

Neorealism: Waltz, *Theory of International Politics*

Neoliberalism: R. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton Princeton University Press, 1984).

Constructivism: Wendt, "Anarchy Is What States Make of It: The Social Construct of Power Politics".

[124] Barkin, *Realist Constructivism*

[125] For an expansion of this argument with specific reference to pluralism and constructivism, see:

S. Guzzini, "A Reconstruction of Constructivism in International Relations", *European Journal of International Relations,* 6, no. 2 (2000).

[126] R.N. Lebow, "Constructive Realism", *International Studies Review,* 6 (2004): 346.

[127] Ibid.

[128] For examples of how synergies exist between realism and constructivism across concepts of roles, power politics, anarchy and self-help behaviours see Kaminski who argues on a thematic level that both employ terms such as 'rules' and 'norms' and Ruggie who comments that both agree on ideational factors that emanate from human capacity and will. Finally, in terms of anarchy, it is noteworthy that realists view it as a motivational factor to assure continued security and Wendt from a constructivist perspective views anarchy as having value depending on 'what states make of it'.

J. Kaminski, "Rethinking Realism and Constructivism through the Lenses of Themes and Ontological Primacy - Introduction-Integrative Pluralism and 21st Century International Relations Theorising", *Croatian International Relations Review,* (2019): 13.

J.G. Ruggie, "What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge", *International Organization,* 52, no. 4 (1998): 856.

Wendt, "Anarchy Is What States Make of It: The Social Construct of Power Politics", 397.

adoption of it as a foundation to research air power's cyber risk is not only logical, but essential if the thesis is to unearth the truths behind this real-world puzzle[129].

Conclusion

Ensuring that this thesis is accessible to not only IR scholars but practitioners, this chapter introduced IR before examining the main paradigms in the context of a focus on air power's cyber risk. In doing so, realism and constructivism were identified as offering intuitive insights. However, with both limited in their ability to shine a light on the research, it was ultimately argued that to achieve the insight the thesis must adopt a pluralist realist-constructivist paradigm.

Reflecting on both this conclusion and the previous assertions on the nature of cyber, it can be concluded that a firm basis for this research into air power's cyber risk has been achieved. Specifically, to explore the topic with depth and rigour the research must adopt a holistic definition of cyber which encapsulates not only digital systems and networks but the people and infrastructure which interact with them. Building from here, the impact of cyber risk on these aspects of air power, and more broadly their impact on the chosen roles of states which utilise air power as a keystone capability, must reflect reality by examining the topic through a pluralist realist-constructivist paradigm. By adopting this it is asserted that the thesis will develop conclusions, observations and recommendations that are not only academically accurate but actionable for practitioners.

[129] For examples of IR scholars with who have adopted or reflected realist-constructivist tendencies in their work, see:
B. Buzan, O. Wæver, and J. de Wilde, *Security: A New Framework for Analysis* (London: Lynne Reinner Publishers, 1998).
J. Mattern, "Why Soft Power Isn't So Soft: Representational Force and the Sociolinguistic Construction of Attraction in World Politics", *Millennium,* 33 (2005).
C Dueck, *Reluctant Crusaders: Power, Culture, and Change in American Grand Strategy* (Princeton Princeton University Press, 2006).
S. Goddard, "When Right Makes Might: How Prussia Overturned the European Balance of Power", *International Security,* 33 (2009).

Part 2: The Causes of Air Power’s Cyber Risk

Chapter 4: The 'First Cause' - Procurement and Reliance on Air Power

Introduction

Having established the foundational concepts in Part 1, Part 2 will introduce the three factors which in combination create air power's cyber risk: states' procurement and reliance on air power, the digitally exploitable nature of modern air power and the existence of credible digital threats to air power. To open the discussion, this Chapter focuses on the first of these.

This cause, states' procurement and reliance on air power, examines the realist assertion that in the contemporary international system states must achieve influence to survive and thrive. In pursuit of this, the discussion justifies how for a significant proportion of states that have the economic capability and imperative to do so, air power can deliver an unparalleled depth and diversity of options. With this uniquely achievable for these states through a relatively small number of digitally enabled air assets, the chapter will show how this comparative advantage has further increased with the digitisation of air power.

To achieve this, the discussion will first explore the contemporary international system. In this, the core IR assumption that states are the principal actors will be acknowledged whilst also accepting a 'post-Westphalian' reality in which non-state actors also play a role. The interaction of this reality with the core IR principles of power and influence will next be explored. Following Hart's argument that power itself has no value, the discussion will demonstrate how it is the state's ability to harness power that is pertinent in meeting the aim of thriving and surviving in the international system[130].

Next considering how in the thesis' realist-constructivist framework states harness influence, the pivotal role played by air power for states whose economic capabilities and imperatives combine to create optimal conditions will be shown.

[130] Hart, "Three Approaches to the Measurement of Power in International Relations", 14.

It will also however be accepted that this is not a blanket conclusion with some states neither positioned nor resourced to become reliant on air power.

Considered reflectively, it will be concluded that where the optimal conditions exist, the vital importance of air power to those states that have the resource and requirement to procure the capability will be underlined. Notably, it will be shown how reliance on the procurement and operation of air power has reached a point at which, if the capability were lost or compromised, roles or even survival may be placed at risk.

The International System

This proposed 'first cause' asserts that the origins of air power's cyber risk are founded on a proportion of states procurement of, and reliance on, air power. In reviewing this statement, the reader's attention may be drawn to cyber and air power. However, at its core is a basic IR assumption: as states are the principal actors of the international system, they must be the focus of IR research.

Though this is often left unchallenged, it is not, as Baylis et al remind us, necessarily true[131]. Increasingly questioned, a shift towards recognising non-state actors and non-traditional security concerns has been witnessed in the 21st century[132]. It is therefore necessary in discussing this 'first cause' of air power's cyber risk to initially step away from air platforms themselves, address a foundational concept in the discussion and justify why it is legitimate for the thesis to pivot around the concept of states.

[131] J. Baylis, S. Smith, and P. Owens, *The Globalisation of World Politics*, vol. 8 (Oxford: Oxford University Press 2020), 16.

[132] C. Eroukhmanoff, "Securitisation Theory," in *International Relations Theory* ed. S. McGlinchey, R. Walters, and C. Scheimpflug (Bristol E-International Relations Publishing, 2017), 104.

The 'Westphalian' System and State Sovereignty

To begin this exploration, one must first consider the origins of the international system. Though predated by concepts of popular or universal sovereignty, its roots are traced to the writings of 17th century thinkers including Grotius[133]. A Dutch scholar, diplomat, and theologian, Grotius's political writings were vast. It is however his thinking on statehood that has relevance to this discussion. Specifically, Grotius asserted that international law should be founded on the idea of territorial sovereignty. This, he contended, would divide the earth into distinct areas, each of which are vested with an equal level of inalienable sovereignty[134].

Though these ideals initially languished, they gained traction in 1648 with the end of the Thirty-Year War and the Treaty of Westphalia. Ending the Holy Roman Empire's claim to universal sovereignty, the Treaty established a commonly accepted system of territorial states which has endured for nearly four centuries[135].

Despite being built on these Westphalian ideals, the current international system was not cemented until 1945 under Article 2 of the United Nations (UN) Charter[136]. Now enshrined in international convention, this asserts that states with defined geographical territories can exercise 'untrampled sovereignty'[137]. Though this offers a clearly defined and internationally agreed parameter from

[133] For the evolution of sovereignty from the individual to the state, see:

M. R. Fowler and J. M. Bunck, *Law, Power, and the Sovereign State: The Evolution and Application of the Concept of Sovereignty* (Pennsylvania: Pennsylvania State University Press, 1995), 11.

For a summary of 'popular sovereignty' and 'universal sovereignty', see:

A. Khan, "The Extinction of Nation-State", *American University International Law Review,* 7 (1992).

[134] For further discussion on Grotius's concepts of state sovereignty being tied to territory, see:

"The Extinction of Nation-State", 202.

K. Haakonssen, "Hugo Grotius and the History of Political Thought", *Political Theory,* 13, no. 2 (1985): 240.

R. Jeffery, *Hugo Grotius in International Thought* (New York: Palgrave MacMillan, 2006), 14.

[135] For comment on the ending of the Pope's influence and the Church reaction to it, see:

R. Jackson, *Sovereignty: The Evolution of an Idea* (Cambridge: Polity Press, 2007), 52.

For further discussion of the Treaty of Westphalia and its importance to the current international system, see:

S.D. Krasner, "Compromising Westphalia", *International Security,* Winter (1996): 115.

J. Havercroft, "Was Westphalia 'All That'? Hobbes, Bellarmine, and the Norm of Non-Intervention", *Global Constitutionalism,* 1, no. 1 (2012): 121.

D. Hassan, "Rise of Territorial State and the Treaty of Westphalia", *Yearbook of New Zealand Jurisprudence,* (2006): 67.

R. Falk, "Revisiting Westphalia, Discovering Post-Westphalia", *Journal of Ethics,* 6, no. 4 (2002): 312.

[136] Specifically, Article 2 (1) asserts that the UN 'is based on the principle of the sovereign equality of all its Members'. Further to this, Article 2 (7) asserts that 'nothing contained in the present Charter shall authorise the UN to intervene in matters which are essentially within the domestic jurisdiction of any state'.

UN, "Charter of the United Nations – Chapter I: Purposes and Principles, Article 2 ", (1945).

[137] L. Gross, "The Peace of Westphalia, 1648-1948", *American Journal of International Law,* 42, no. 1 (1948): 20.

which this thesis can be based, sovereignty is not in reality as neatly packaged as the UN Charter might suggest.

Explored by Krasner, he concludes that contrary to many observations sovereignty cannot be considered an 'analytical assumption or…taken-for-granted structure'[138]. Rather, he argues that when examined the properties of territory, recognition, autonomy and control that form the bedrock of state sovereignty are frequently compromised. Though on occasion such compromises occur through force, Krasner highlights that it is more often witnessed through states voluntary involvement with international agreements, treaties, or membership of transnational organisations. In accepting the limitations these impose, states in turn relinquish part of their sovereignty. As a result, despite the UN grand assertion of 'untrampled sovereignty' the concept is neither static nor unbending[139].

This questioning of state sovereignty can be further supported by other international concepts that have emerged in the late 20th and early 21st century. Notable amongst these is R2P. Championed by UN Secretary General Kofi Annan from the early 2000s, R2P asserts that the UN Security Council (UNSC) can authorise the compromise of a state's sovereignty to restore international peace and security[140]. Supporting Krasner's assertion that the contemporary international system undermines any argument for 'untrampled sovereignty', R2P undoubtedly brings the core premise of the 'Westphalian' system into question.

However, in reflecting on Krasner's argument and R2P one must also recognise that despite the challenges they offer both acknowledge the importance of sovereignty. This is achieved by the fact that Kranser dedicated an entire book to

[138] S.D. Krasner, *Sovereignty: Organised Hypocrisy* (Princeton Princeton University Press, 1999), 220.

[139] For a summary of Krasner's argument, see:
Ibid.

[140] R2P was championed by Secretary General Kofi Annan in response to the atrocities committed in the Balkans and Rwanda. For further depth on R2P, see:
UN, "Charter of the United Nations – Chapter Vii: Action with Respect to Threats to Peace, Breaches of the Peace and Acts of Aggression, Article 39 ", (1945).
"2005 World Summit Outcome Document ".
Annan, "We the Peoples: The Role of the United Nations in the 21st Century ".
Evans and Sahnoun, *International Commission on Intervention and State Sovereignty (Iciss), the Responsibility to Protect*

its discussion and R2P requires the UNSC to approve any compromise of it[141]. Based on this, one can conclude that state sovereignty, and the 'Westphalian' system which introduced it, remain fundamentally central to understanding the contemporary international system.

The State-Centric Argument

One could therefore conclude that state-focused research which pivots on the centrality of sovereignty and the 'Westphalian system' is not just valid, but the only logical foundation for IR scholars. Though defensible, its pertinence is enhanced when applied to realism, an element of this thesis' pluralistic framework, and air power.

Built on a lineage of scholastic work reaching back to Thucydides, the international system is for realists characterised by its anarchic nature[142]. This is created, realists argue, by a combination of man's egotism and the lack of legitimate government above the state. Driving states as man's international manifestation to assure their survival through any means, a reality is created in which states are the main actors and power is the main theme[143].

Building on this, contemporary realists continue to support the primacy of states. Built in large part on Morgenthau's 1948 book *Politics Among Nations*[144]*,* these arguments would later assume a more distinct form in neorealists assertions such as Waltz's 1979 book *Theory of International Politics*[145]. Through these developments, one can view the contemporary realist state-centric theory as built on three principles: international politics as a bounded domain, controlling law-like regularities existing within it and, to understand the domain, the existence of observed regularities.

[141] Krasner, *Sovereignty: Organised Hypocrisy*
[142] P. J. Ahrensdorf, "Thucydides' Realistic Critique of Realism", *Polity,* 2, no. Winter (1997): 232.
[143] Korab-Karpowicz, *Political Realism in International Relations - Stanford Encyclopaedia of Philosophy*.
[144] For Morgenthau's book, see:
Morgenthau, *Politics among Nations: The Struggle for Power and Peace*
For an analysis of Morgenthau's discussions on the primacy of states, see:
T.J. Volgy et al., Major Powers and the Quest for Status in International Politics: Global and Regional Perspectives (New York: Palgrave MacMillan, 2011), 2.
[145] Waltz, *Theory of International Politics*

Providing a final key to this theoretical approach, and delivering a means of explaining the observed regularities, Waltz employs the oligopolistic nature of economics as an analogy. Applying this to the international system, he asserts that the prime influences or 'units' remain states. Therefore, when establishing any hierarchy states must be at the top[146]. A logic later developed by Gilpin, it can be asserted that the international system, which in Gilpin's view is concurrently anarchic and highly ordered, rests on a distribution of power among a relatively small number of states[147].

In considering these themes, one is presented with an unequivocal argument that states must be the central theme of IR. Enhancing this is the thesis' focus on advanced air power and the role the capability plays in assuring a state's survival. With such capabilities principally operated by states, and their role being the prime means of excerpting power and control over anarchy, there is, it can be concluded, no option for this thesis other than to make states its pivotal focus.

The Counter State-Centric Argument

Though this conclusion is persuasive, it is also acknowledged that global changes have in the last century seen a rise of transnational influences and non-state actors. In making this statement, it is recognised that throughout the existence of the 'Westphalian system' non-state actors have played a significant role in the international system[148]. However, with contemporary non-state groups ranging from the 'third sector' of self-governing socially focused organisations, to violent and criminal non-state groups and global corporations, their collective challenge to state-dominance is increasingly diverse and potent[149]. Balanced against the

[146] See Waltz's *Theory of International Politics* for a full development of this argument.
Ibid.

[147] For a full discussion of these arguments, see:
R. Gilpin, *War and Change in World Politics* (Cambridge Cambridge University Press, 1981), 28-29.

[148] For example, the British East India Company, and other similar non-state actors such as the Hudson Bay Company, were corporate in form but exercised significant power across large areas of the globe including the Indian sub-continent and North America.
P. Lawson, *The East India Company: A History* (London: Routledge, 1993).
E. Blakemore, "How the East India Company Became the World's Most Powerful Business", *National Geographic* 2020.

[149] For an introduction to the non-profit 'third sector', see:

limitations of states expressed by Krasner in his discussion of sovereignty, there is a valid argument that for this thesis to adopt a purely state-centric approach would be ill-advised[150].

Considering first transnational influences, academic challenges to the traditional state-centric view have been inspired since the 1990s by the Copenhagen School. Underpinned by liberal ideals, scholars including Buzan and Waever have championed an 'expansionist' agenda arguing for a more comprehensive approach to IR[151]. In this, human security and not security of the state is recognised as the primary factor[152].

Developed from a lineage including US President Franklin's famous 1941 'Four Freedoms' speech, this adjustment of IR has been sufficiently successful as to be adopted beyond academia[153]. A prominent example is the UN Development Programme (UNDP) which in 1994 called for a renewed impetus behind human security and freedoms from fear and want[154]. Making the individual, not the state, the referent object, these arguments provide emphasis to the 'expansionist' movement.

Acting alongside these, and arguably more pertinent to this research, are an expanding array of non-state actors. Though often difficult to define, these are in the UN's view any 'individual or entity…[which is] not acting under the lawful authority of a state'[155]. Incredibly diverse, the most high-profile of these are multinational corporations. Existing in all parts of the global economy from retail to technology, they may appear non-threatening but can, nonetheless, be seen

L.M. Salamon, "The Rise of the Non-Profit Sector", *Foreign Affairs,* 73, no. 4 (1992).
For an introduction to non-state violent and criminal ground such as Al-Qaeda and the Russian Bratva 'mob', see:
B. Berti, "Violent and Criminal Non-State Actors," in *The Oxford Handbook of Governance and Limited Statehood* ed. A. Draude (Oxford: Oxford University Press, 2018).
For an introduction to contemporary global corporations, see:
G. Jones, *Multinationals and Global Capitalism* (Oxford: Oxford University Press, 2005).

[150] Krasner, *Sovereignty: Organised Hypocrisy*

[151] The Copenhagen school, an academic movement with links to the Copenhagen Peace Research Institute (COPRI), is primarily associated with the works of Buzan, Wæver and de Wilde. Texts which defined the thinking of the Copenhagen School include:
Buzan, Wæver, and de Wilde, *Security: A New Framework for Analysis*
B. Buzan, *People, States and Fear* (Brighton: Wheatsheaf Books, 1983).

[152] R. Ullman, "Redefining Security", *International Security,* 8, no. 1 (1983).

[153] F.D. Roosevelt, "Four Freedoms Speech", *American Rhetoric: Top 100 Speeche,* (1941).

[154] O. Gomez and D. Gasper, "Human Security", ed. UNDP Human Development Report Office (United Nations 2020), 1.

[155] UN, "Security Council, Resolution 1540", (2004).

as 'obliterating spatial lines…and making nonsense of geographical demarcations'[156]. Reducing states to little more than 'economic units', the Westphalian model and the associated realist assertions on the state have, in this view, been replaced by a pragmatic appreciation of global markets[157].

A further and arguably more pertinent non-state example to this research are violent non-state actors. Testing the traditional stance of IR scholars across all paradigms to focus on state-on-state concerns, their growth has created a new form of conflict that is not limited by geography. Blurring the lines between crime, terrorism and irregular warfare, groups including Al-Qaeda and their affiliates who perpetuate asymmetric conflict are often well-resourced and driven by ideology not territory[158].

Individually concerning, in combination these contemporary developments have become commonly referred to as representing a 'beyond Westphalian' reality[159]. When examined under this banner, it is evident that states are no longer the only actors in the international system. An argument explored by Breslin and Nesadurai, there is a risk, they conclude, that any IR research which ignores this fact and dismisses the role of non-state influences will only achieve a partial understanding of the world[160].

Though convincing, others including Falk's assert that whilst the Westphalian system may be diminished, the power of states remains formidable. Expanding on the argument, he concludes that though the environment has changed, the most likely development is not a demise of the state. Rather, the reality is one in

[156] This statement was made by:
O. Schachter, "The Decline of the Nation-State and It Implications for International Law", *Columbia Journal of Transnational Law,* 36 (1998): 8.
The argument Schachter presented is supported by:
V. Cable, "The Diminished Nation-State: A Study in the Loss of Economic Power", *Daedalus,* 124, no. 2 (1995): 23.

[157] Kindleberger makes this argument noting as early as 1969 that globalisation has made the nation-state no more than an economic unit.
C. Kindelberger, "American Business Abroad," in *Globalisation, the New Economy and Regionalisation'*, ed. R. Sugden and J. R. Wilson (GaWC Research Bulletin, 1969; reprint, 2001).

[158] This argument on the new nature of non-state centric conflict is taken from Chapter 2 of:
N. Ezrow, *Global Politics and Violent Non-State Actors* (London: Sage Publications, 2017).

[159] D. Croxton, "The Peace of Westphalia of 1648 and the Origins of Sovereignty", *The International History Review,* 21, no. 3 (1999): 569.

[160] S. Breslin and H.E.S. Nesadurai, "Who Governs and How? Non-State Actors and Transnational Governance in Southeast Asia", *Journal of Contemporary Asia,* 48, no. 2 (2018): 188.

which emerging globalism and economic trends create political communities which share power with, but do not replace, the state[161]. A logic associated with the less stark term 'post-Westphalia' these arguments represent a more probable version of the contemporary reality.

A State-Centric (but not Blinkered) Focus

In reviewing the above debate, Miller notes several substantive problems with the 'expansionist' movement. Specifically, he concludes that much of the arguments are based on normative grounds with little empirical evidence to support the degradation in the role of the state[162]. Given this, though the concept of protecting the individual as the referent object may be ideologically preferable, the reality, even in a post-Westphalian world, is that realist assertions on state primacy, anarchy and the centrality of power remain unchanged. Because of this, the state must, it is concluded, remain the focus of not only IR but this thesis.

Whilst this position is defendable, it is also recognised that the non-state challenges cannot be wholly dismissed. Though not creating a shift so significant as to legitimise the 'beyond Westphalia' label, they have led to a transition which is close to a 'post-Westphalian' reality. In accepting this, it is further concluded that although remaining state-centric the thesis will also, especially in its explorations of air power's cyber threats and vulnerabilities, not be blinkered and ensure that non-state influences are, where relevant, examined.

Power and Influence

Having established the nature of the international system and the primacy of states within it, it is necessary to understand how states harness power, exert influence and what motivates them to do so. From this, the thesis will explore how states meet these demands by using military 'means' to achieve political 'ends' and, within this, the unique role of air power. Ultimately, the discussion will

[161] Falk, "Revisiting Westphalia, Discovering Post-Westphalia", 350.
[162] B. Miller, "The Concept of Security: Should It Be Redefined?", *Journal of Strategic Studies,* 24, no. 2 (2001): 27.

provide a thorough understanding of the proposed 'first cause' of air power's cyber risk: states procurement of, and reliance on, air power.

The Concepts of Power and Influence

To begin this exploration, it is first necessary to understand the concepts of power and influence. At the core of this is the fundamental realist concept of power which, in the context of states, concentrates on one question: 'power over whom, and with respect to what?'[163].

Despite representing a long-held interest for IR scholars, Morgenthau cautions that attempting to answer it has become one of the disciplines most challenging and controversial topics[164]. Equally, with it sitting at the centre of not only IR but the nature of human existence, it presents 'as ancient and ubiquitous [a topic] as any that social theory can boast'[165]. Because of this, it is unsurprising that Nye likens power to the weather: something everyone depends on and discusses, but few understand[166].

Acknowledging this warning it is prudent in examining how states achieve influence through power to first consider the concept in its most literal sense. Specifically, power can be defined as the means, ability, and capacity to achieve something[167]. Transposed into discussions of IR and the state-centric system, power must be taken to be the means through which states achieve desired outcomes.

Despite this apparent ease of definition, such an interpretation is veneer deep with it remaining a contested concept[168]. Discussing the challenges this invokes, Dahl recognised as early as the 1950s that the issue is fundamentally unsolvable. In making this judgement he commented that any attempt to form a formal

[163] Jablonsky, "National Power", 34.
[164] Morgenthau, *Politics among Nations: The Struggle for Power and Peace* 13.
[165] R.A. Dahl, "The Concept of Power", *Behavioural Science,* 2, no. 3 (1957): 201.
[166] J. S Nye, *Soft Power: The Means to Success in World Politics* (New York: Perseus Books Group, 2004), 1.
[167] J. B. Condliffe, "Economic Power as an Instrument of National Policy", *The American Economic Review,* 34, no. 1 (1944): 306.
[168] F. Berenskoetter and M. J. Williams, "Thinking About Power," in *Power in World Politics* ed. F. Berenskoetter (London: Routledge, 2007), 12.

definition of power which meets the needs of a particular research problem will inevitably diverge from all other areas of research[169]. Through this conclusion, Dahl warns academics not to seek 'a single, consistent, and coherent 'Theory of Power' [170].

In response, one of the most pragmatic attempts to define the concept is found in Hart's 1976 article[171]. Acknowledging the limitations highlighted by Dahl, Hart does not seek a single definition. Rather, he measures the indicators of power by dividing them into whether states seek control over resources, actors or events and outcomes[172]. Offering insight into not only power but how power creates influence, Hart importantly underlines one of the few constants in IR: the assertion that 'power is relative, not absolute'[173]. From this we can conclude that power itself has no value. Rather, it is a state's motivation and subsequent ability to harness power through influence over either resources, actors or outcomes and events that is pertinent.

The Motivation to Harness Power

Reflecting on this initial conclusion, the next step in exploring the criticality of air power is to confirm the factors that motivate states to harness power through influence. To achieve this within a realist-constructivist framework, it is necessary to examine the individual components before considering how the 'separate but interlocking pieces' link together[174].

[169] Dahl, "The Concept of Power", 202.
[170] Ibid.
[171] Hart, "Three Approaches to the Measurement of Power in International Relations".
[172] In the first, control over resources, Hart discussed the concept in terms of empirical judgements on control over aspects such as military expenditure, gross national product, etc. In the second, Hart illustrates the concept of control over actors by borrowing Dahl's definition of power which gauges it in terms of the ability of 'A' to get 'B' to do something. In the final category, outcomes and events, Hart gauges power in terms of what is achieved, and whether this meets the states intent, rather than the resources used to achieve it.
Ibid., 292.
Dahl, "The Concept of Power", 202.
[173] Jablonsky, "National Power", 37.
[174] Lebow, "Constructive Realism", 346.

Realism

Beginning with realism, scholars present motivation in terms of egotism and self-interest. In this context, both 'individual man and men aggregated into states…[are motivated to] seek, maintain or increase power'[175]. A sentiment originally articulated by Thucydidies, these drivers are viewed as overcoming any moral principle in all situations. Leading man to pursue the 'aggrandisement offered by superior strength', Thucydides and those who follow his philosophies conclude that the weak will always be subject to the strong[176].

Underpinned by the allied principle that all human activity is fundamentally focused on survival, these realist themes have continued into the contemporary form of neorealism. Though changing focus in neorealism from power being its own ends to power being a means to survival, the basic motivational realities remain constant[177]. Specifically, states recognise that to achieve their intent to survive they must hold a sufficient share of relative power when compared to their adversaries.

Taken in this context, states are driven to attain power and convert that power into influence to survive. Logic therefore dictates that a state will seek the most potent means to achieve the desired ends. If, as explored below, air power offers this potency above all other means, states will be drawn towards its procurement and, thereafter, become reliant on the capability.

[175] Jablonsky, "National Power", 34.

[176] For the quote, see:
Thucydidies, *The History of the Peloponnesian War*, trans. R. Crawley (New York: Dutton and Company), 1-76.
For a discussion on motivation as expressed by classical realism, see:
Korab-Karpowicz, *Political Realism in International Relations - Stanford Encyclopaedia of Philosophy*.
For detail on Thucydidies thinking, see:
Thucydidies, *The History of the Peloponnesian War*, 1-76.

[177] It is further noted that this development of neorealism has also been nuanced through the development of defensive and offensive realism. These will not be discussed further. However, for depth on offensive realism, see:
Forde, "Varieties of Realism: Thucydides and Machiavelli", 372.
For depth on defensive realism, see:
Mearsheimer, *Structural Realism' in International Relations Theories: Discipline and Diversity* 83.
For depth on both offensive and defensive realism, see:
S.E. Lobell, "Structural Realism / Offensive and Defensive Realism," in *Oxford Research Encyclopaedia of International Studies* (Oxford: Oxford University Press, 2010).

Constructivism

Though realism explains states' base level motivations, it does not unpack the complexities of the international system. To achieve this, we must turn to the constructivist element of the pluralistic framework. Whilst criticised by some theorists as an 'empty vessel' which fails to prescribe a social ontology, constructivists have since the 1980s challenged established IR thinking[178]. Arguing that international politics is historically contingent rather than naturally occurring, the paradigm's principles as summarised by Wendt and developed by the subdiscipline of role theory, explain how the contemporary international system has been built on top of realist desires. In reflecting on this, one gains insight into how constructivism cements the motivations of states to pursue power and influence in specific ways[179].

Using role theory to illustrate the argument, we note that beginning as a theatrical metaphor it asserts that as actors are constrained by 'parts', the motivations of states can be predicted by 'roles'. Therefore, though the realist instinct is to survive, historically contingent factors necessitate states to assume roles in the international system. Having done so, their status and ultimately survival become interlinked forcing states to be motivated to 'act their part'[180].

Socially implanted above the realist desire to survive, this constructivist characterisation explains why states are motivated to procure and operate military capabilities which allow them to maintain their roles. This is because, for example, a great power without the military capability to project global influence will quickly reduce in role and status to that of a regional power. With the concept

[178] For criticisms of constructivism, see:
Flockhart, "Constructivism and Foreign Policy," 81.
For an understanding of the origins of constructivism, see:
Onuf, *World of Our Making*.

[179] Wendt's three principles of constructivism are: all states act towards others based on the meaning that they have for them; states assume roles to guide these interactions; and international organisations stabilise these interactions allowing states to pursue role-based interests. For a full description, see:
Wendt, *Social Theory of International Politics*, 399.

[180] Holsti is credited with establishing the modern IR role theory. Notably, see:
Holsti, "National Role Conceptions in the Study of Foreign Policy".
For a discussion on Hosti's work, see:
Biddle, "Recent Developments in Role Theory", 68.

of survival for all states naturally entwined with the role to which they have become motivated, they will seek to avoid this relative decline at all costs. Therefore, the question this thesis must address is whether air power is a pivotal capability relied on by states to assure the maintenance of their role and status.

Realist-Constructivism

The above narrative illustrates why both realism and constructivism are relevant to this thesis. It also introduces how constructivism can be characterised as being built on top of realist tenets. However, as Sterling-Folker identifies, even though the argument for combining the two can be made, 'the difficulty lies in how to accomplish the goal'[181].

A question that has generated scholarly debate, some academics contend that the process of finding a path towards realist-constructivism is limited by those who fail to understand paradigms outside of their narrow world view[182]. It is in taking such a polarised position that academics can form, in Lebow's estimation, stereotypes that prevent the recognition of synergistic advantages in combining paradigms[183].

The first step in breaking down these barriers for realist-constructivism is, in Barkin's view, to refute the assertion that constructivism is an IR paradigm equivalent to that of realism or liberalism[184]. A position encouraged by textbooks and the 'paradimic castles' they create, constructivism is often set up in the pedagogy of IR as a standalone paradigm whose concepts are mutually exclusive of realism. However, in adopting this position, as many scholars have, the stereotypes Lebow refers to obscure compatibilities that can enrich realism[185].

[181] J. Sterling-Folker, "Realist-Constructivism and Morality", *International Studies Review,* 6, no. 2 (2004): 341.
[182] This argument on the limitations of academics viewing paradigms as natural opponents and not recognising the value of finding synergies has been made by several academics. Notable discussions on this topic include:
S.J. Barkin, "Realist Constructivism", ibid.5, no. 3 (2003): 325.
Lebow, "Constructive Realism", 346.
[183] "Constructive Realism", 346.
[184] S.J. Barkin, *Realist Constructivism: Rethinking International Relations Theory* (Cambridge: Cambridge University Press, 2010), 2.
[185] Ibid.

To begin this 're-education' of constructivism, one must initially breakdown the 'castle walls' and recognise the concept as a 'set of assumptions about how to study world politics…[rather than] a set of assumptions about how politics work'[186]. Adopting this perspective, constructivism and the tool sets it offers such as role theory allow a better appreciation of the international system and revisit realism's thinking on motivation[187]. This assertion is illustrated by Lebow in his article *Thucydides the Constructivist*. In this he argued that whilst at a superficial level Thucydides appears purely realist, a deeper analysis identifies that his exploration of the relationship between nonos (convention) and phusis (nature) finds the existence of analytical tools which are strongly reflective of contemporary constructivism[188]. Therefore, though realist in his foundation, one could identify Thucydides as the first realist-constructivist.

Once this contention that constructivism is not a paradigm but a set of research methods is adopted, its utility as an adjunct to realism becomes clear[189]. However, in doing so, a specific issue of reconciling realisms focus on power becomes evident. In Jackson and Nexon's view, for example, this question leaves a distinct uncertainty in the realist-constructivist approach. Specifically, by forcing the combination the pluralistic approach becomes either constructivism offering a 'gloss on realism…or realism [being] endogenous to constructivism'. In neither version, however, do Jackson and Nexon view realist-constructivism as offering value to IR[190].

To address this, one can reflect on Barkin's contention that power and the influence it creates is an ever-present concept that takes differing forms depending on the socio-political circumstances. Accommodating the realist's centrality of power, this identifies that it is by understanding and employing the constructivists tool sets against realist conceptions of power that scholars can

[186] Barkin, "Realist Constructivism", 336.
[187] Ibid., 338.
[188] R.N. Lebow, "Thucydides the Constructivist", *The American Political Science Review,* 95, no. 3 (2001).
[189] For further depth on this argument, see:
Barkin, "Realist Constructivism", 338.
Guzzini, "A Reconstruction of Constructivism in International Relations", 150.
[190] P.T. Jackson and D.H. Nexon, "Constructivist Realism or Realist-Constructivism", *International Studies Review,* 6 (2004): 339.

understand how it is moulded and directed in the international system[191]. Expanding on this, Mattern concludes that the value of realist-constructivism is therefore in its utility as a tool set through which to investigate power[192].

Reflecting on this characterisation of realist-constructivism, the motivation of states to harness power through influence remains unchanged from the above conclusions on realism. Specifically, if air power offers potential potency above all other means, states will be drawn towards its procurement and, thereafter, become reliant on it. However, in understanding how this realist desire to survive and thrive will be achieved, we must also explore how it is overlaid by, and explained through, the constructivist tool set. By doing so with role theory as the key focus, the thesis is offered as a means, as expressed above, to not only understand how power manifests itself in the international system but also how the procurement of air power can be designed to prevent or manage relative decline.

Therefore, collectively these 'interlocking pieces' of realism and constructivism offer the thesis a viable means through which to understand why states are motivated to harness power. In doing so, a basis is delivered through which the larger IR puzzle of states reliance on air power and, ultimately, the causes and consequences of air power's cyber risk can be addressed[193].

Harnessing Power

Considering the above discussion of power and influence, and what motivates states to pursue them, we are shown that in developing, procuring, and operating military means states are not interested in the capabilities themselves. What they are motivated to achieve is a sufficient level of control and influence. In delivering this thesis, a key question to ask is therefore whether air power is unique in its ability to deliver this influence. If it is, it would be logical to conclude that states

[191] Barkin, "Realist Constructivism", 325.
[192] J.B. Mattern, "Power in Realist-Constructivist Research", ibid.6, no. 2 (2004): 345.
[193] Lebow, "Constructive Realism", 346.

are not only likely to procure air power but will become reliant on it as a key strategic asset.

To address this, one must first examine air power through the context of how states harness resources to achieve influence and, in this, what role the capability plays. The answer to the initial part of this question is, Nye argues, through one of three ways: the use of a 'stick' to threaten or coerce, the use of 'carrots' to induce and encourage or, finally, the use of 'attractions' to make others want to act in a particular manner[194]. Whilst this represents a broad academic discussion, these fundamental concepts can be most clearly conceptualised through the instruments of power and, more specifically, how each is harnessed in the form of hard, soft, and smart power.

Instruments of Power

Initially considering the instruments of power, these have traditionally been defined as diplomatic, economic, and military. In the first, the diplomatic instrument, we are presented with a form of influence focused on 'the art of persuasion'[195]. Firmly in the 'carrot' category, diplomacy remains, despite the increasing role of non-state actors, the purview of states[196].

Though well-established, diplomacy is limited without the backing of the other instruments which lend it persuasive means. The first of these is the economic instrument. Straddling the 'stick' and 'carrot' categories depending on its employment, the economic instrument was traditionally focused on the ability to convert natural or human resources into economic activity that would 'buttress the military strength of the state'[197].

[194] Nye, "Public Diplomacy and Soft Power", 94.

[195] I. Salama, "Human Rights Diplomacy from a Un Perspective: A Complement to Advocacy," in *Human Rights Diplomacy: Contemporary Perspectives* ed. M. O'Flaherty (Netherlands: Brill Nijhoff, 2011), 129.

[196] For a discussing on the nature, capacity, and role of the diplomatic instrument of national power, see:
C. Freeman et al., "Measuring Diplomatic Capacity as a Source of National Power", *Review of International Affairs,* 40, no. 1 (2020).
For a discussion on 'public diplomacy' and the increased role of non-state actors in an instrument of power, see:
G. Lee and K. Ayhan, "Why Do We Need Non-State Actors in Public Diplomacy?: Theoretical Discussion of Relational, Networked and Collaborative Public Diplomacy", *Journal of International snd Area Studies,* 22, no. 1 (2015).

[197] Condliffe, "Economic Power as an Instrument of National Policy", 305.

It is recognised, however, that in the last century economies have developed in line with globalisation and the rise of multinational companies. In response, academics including Nye argue that the world has reached a point at which the state is no longer relevant in discussions of economic power[198]. Challenging this, others including Lash suggest that the demise of the state is 'grossly exaggerated'[199]. An assertion underlined by the continued use of politically motivated economic sanctions and embargoes, states appear to persist as central to the economic instrument[200].

Despite the diplomatic and economic instruments remaining relevant and largely state-centric, realist scholars argue the realities of security, competition and war prove that both will ultimately fail[201]. When this occurs, it will, realists contend, be the military instrument that becomes paramount in harnessing resources, delivering control, and achieving the influence that assures the survival and growth of states. Therefore, operating within the realist paradigm, we must conclude that though the diplomatic and economic instruments have value, they will in state-centric terms always be subordinate to the military instrument of power.

Though IR scholars of other persuasions may contest this view, this military primacy has been evidenced throughout history. Discussed by Jablonsky, military strength has, he argues, with credible reason always been the 'ultima ratio' of power[202]. This is proven by the simple fact that a state's defeat in war will signal its decline, while victory usually heralds a rise of power[203].

[198] For example, Keohane and Nye suggest that 'burgeoning social and economic transactions [are] creating a world without borders'. This will, they argue, see multinational corporations, transnational social movements, and international organisations lead with the state becoming thought of as an economic unit.
Keohane and Nye, *Power and Interdependence*, 3.

[199] W.H. Lash, "The Decline of the Nation State in International Trade and Investment", *International Trade and Investment,* 18 (1996): 1025.

[200] For example, see the 'Current Trade Sanctions' list published by the UK Government as an example of the continued active use of sanctions on a nation state level.
UK, "Current Trade Sanctions, Including Arms Embargoes and Other Restrictions", ed. Department for International Trade (Great Britain HM Government 2020).

[201] For an expansion of this realist argument on the importance of the military instrument, see:
Mearsheimer, *The Tragedy of Great Power Politics* 97.

[202] Jablonsky, "National Power", 35.

[203] Ibid., 45.

Given this logic, there is a strong argument that having identified states as the key actors in the contemporary international system, it must be their employment of the military instrument that is central to any discussion of how power is translated into influence. Within this, it must further be the means of delivering influence, namely military capabilities, that are pivotal to the argument. To explore this issue in a systematic manner, and gauge whether the capability of air power offers a disproportionate ability to deliver influence, it is necessary to divide the discussion into the key themes of how power is harnessed: hard, soft, and smart power.

Hard Power

The first of these, hard power, is the most obviously linked to the military instrument. Employed to coerce or induce through the threat or use of force, it is commonly perceived to be the raison d'être of all military organisations[204]. Given this, one might argue that no one military capability deserves specific consideration but all, in their niche, deliver unique and equally important resources.

Though a potentially valid argument, a review of the five generations of warfare confirms that throughout history decisive strategic effect has routinely been achieved through a small selection of advanced capabilities[205]. Of these, air power has for over a century been the most impactful.

Neither instantaneous nor without controversy in its' rise, air power was pioneered by the German use of Zeppelin Airships to attack the UK in January 1915. In this early evolution, air power would be considered a minor capability with limited strategic effect[206]. This view would, however, change during the Second World War with air power becoming indispensable to the modern

[204] For example, UK Military Doctrine defines Hard Power as actions intended to 'coerce opponents to adopt a particular course of action, which they would not otherwise choose themselves'.
UK, "Joint Defence Doctrine 0-01 Uk Defence Doctrine", 3.

[205] For a discussion on the evolution of warfare in the five generations, see:
C. Băhnăreanu, "The Evolution of Warfare from Classic to Hybrid Actions", *Strategic Impact,* 2 (2015).
W.S. Nightengale, "The Changing Face of War: Into the Fourth Generation", *Marine Corps Gazette,* (1989): 22.

[206] Stephenson, *Zeppelins: German Airships 1900?* , 13.

battlefield. This movement towards its primacy within the military instrument was succinctly summarised in 1954 by Montgomery who stated that 'if we lose the war in the air, we lose the whole war and lose it quickly'[207].

Despite scholars including Pape questioning the strategic value of air power, and acknowledging that other capabilities including the nuclear deterrent also play key roles, predictions of its future pre-eminence made by early air power theorists including Douhet and Marshall have been proven[208]. Demonstrated repeatedly throughout the last century, some of the most prominent examples have included the US 1965 Operation Rolling Thunder in Vietnam, and the UK 1982 Black Buck raids in the Falkland Islands[209]. Though in these and other similar examples it is acknowledged that the combat effectiveness of air power might have fallen short of expectations, they have met Pape's criteria for coercive success in terms of strategic effectiveness.

For example, though the Black Buck raids would only inflict modest and reparable damage to the runway at Stanley Airfield being used by the Argentinians, its strategic value was convincing the Argentinians that the UK could use air power to target their mainland. In doing so, Argentina diverted air assets to homeland defence allowing UK operations in the Falklands to continue with a reduced risk from the air[210]. Based on this, it can be concluded that despite arguments on the

[207] Montgomery, "The Role of Science in Warfare of the Future".
Staff Writer, "Field Marshal Montgomery – Obituary'", *New York Times* 1976.

[208] Pape's statement does not suggest that he dismisses the value of air power. Rather, he argued that when its value is gauged on combat effectiveness alone its apparent impact can be misinterpreted. To illustrate his point, he cites the incendiary bombing of Japanese cities during the Second World War. These he highlights were hailed as successful due to the damage they caused. However, in truth, the raids failed to achieve meaningful impactful because of the Japanese Governments willingness to accept the civilian loss of life.
Pape, *Bombing to Win: Air Power and Coercion in War*
Douhet asserted that air power (specifically strategic bombing) could in isolation be a deciding factor.
C.G. Segrè, "Giulio Douhet: Strategist, Theorist, Prophet?", *The Journal of Strategic Studies,* 15, no. 3 (1992): 352.
Taking a middle ground Marshall later argued that integrated air capabilities would be the decisive factor in all future operations.
B.S. Lambeth, *The Winning of Air Supremacy in Operation Desert Storm* (Santa Monica: RAND, 1993).
For a broader discussion on the role of the nuclear deterrent as a strategic capability, see:
Payne, *Deterrence in the Second Nuclear Age* 1.

[209] The US led Operation Rolling Thunder in the Vietnam conflict during 1965 was intended to 'stop the infiltration of personnel and supplies [into the south] by the Democratic Republic of Vietnam'. In achieving its aim, the air operation prolonged US ground operations in the country.
Frankum, *Like Rolling Thunder: The Air War in Vietnam, 1964-1975*, 3, 65.
The UK led Black Buck in 1982 raids saw the Vulcan aircraft used for 'the longest bombing mission ever attempted' to coerce Argentina into withdrawing air assets to defend its homeland. This allowed the UK to achieve air superiority over Argentina and successfully land ground forces in the Falkland Islands.
Posey, "Air War in the Falklands", 75.

[210] G. Sheffield, "From San Carlos to Stanley: The Falklands Land/Air Operation", *International Relations,* 20, no. 3 (2006): 373.

limitations of air power, the strategic effect it has had on the outcome of conflicts has proven early predictions of dominance over the land and maritime operating domains.

These examples demonstrate air power's historical hard power dominance. However, its importance is arguably set to grow as a fifth generation of network enabled warfare continues to be developed. A prediction underlined by NATO's recognition of a cyber domain[211], these advances have redefined operations allowing air platforms to achieve greater hard power effect[212].

This transformation of air power was initially demonstrated in the first Gulf War of 1990 to 1991. Illustrating an unrivalled ability to deliver hard power, the opening elements of the Gulf War were described by Mason as marking the 'apotheosis of 20th century air power'[213]. Going further, Mason commented that sitting at the heart of the Coalitions Gulf War experience, air power had by harnessing digital enablement emerged as the unrivalled source of hard power[214]. Making it in Hallion's view stand out as a 'major transformation in the nature of warfare', air power not only came of age but dominated the battlefield[215].

Building on this, air power has in the 21st century also shown a unique ability to deliver strategic intent when, for economic or political reasons, the resource intensive deployment of land forces is not viable. Illustrated by NATO's 2011 air-led intervention in Libya, and the US led Coalitions 2014 to 2017 air campaigns against the Islamic State of Iraq and Syria (ISIS), it is expected that such claims for air power's dominance will continue to be proclaimed[216].

[211] For an overview of NATO's declaration of a 'cyber domain', see:
NATO, "Cyber Defence ", (2019).
G. A. Crowther, "The Cyber Domain", *The Cyber Defense Review,* 2, no. 3 (2017): 63..

[212] Lambeth lists air powers traditional strengths as speed, range and flexibility. It is argued that new technologies have not removed these, but rather offered revisions and enhancements as to how air power can be employed. In equal measure, however, new digital vulnerabilities have been introduced providing means to undermine air power's strengths.
Lambeth, *American Air Power* 8.

[213] R.A. Mason, "The Air War in the Gulf", *Survival,* 33, no. 3 (1991): 225.

[214] Ibid.

[215] For an expansive discussion of the Air War in the fully in 1991, see:
Hallion, *Storm over Iraq: Air Power and the Gulf War* 1.

[216] It is acknowledged that both the 2011 air-led NATO intervention in Libya and the 2014-17 Coalition air campaign against Daesh required host nation land forces to meet objectives. It is further noted that both also witnessed the limitations of air power in terms of its ability to achieve decisive effect. However, in both, the states supplying the air power achieved their strategic goals without having to deploy large ground forces.
Mueller, *Precision and Purpose: Airpower in the Libyan Civil War*
Fishel and Stein, "Lessons Learned from the Air War against the Islamic State".

Already impressive in the context of the 'fifth generation of warfare', air power's ability to deliver influence through hard power can, with the advent of 'fifth generation aircraft', be expected to grow[217]. Harnessing technology to the point at which air platforms are integrated with and fully exploiting digital networks, the capability continues to develop at speed[218]. Translating into strategic effect, states can now rely on relatively small fleets of manned and unmanned aircraft to achieve strategic impact across numerous defence tasks: something which neither land nor naval forces can match. Cementing air power's dominance in the sphere of hard power, it can for those states able to afford fifth generation air power be intuitively regarded as a keystone of the strategic delivery of hard power.

This conclusion confirms why in the context of hard power air power is likely to be procured and relied on. Hard power is not, however, the only form of power. An assertion supported by Wilson, he argues that those who blindly adhere to hard power routinely 'ignore or simply subsume elements of national power that lie outside their traditional purview'[219]. Developing this, UK Doctrine notes that 'while hard power may offer a solution to one problem, it may undermine attempts to solve others'[220]. Air power must therefore demonstrate broader utility if the argument that states are likely to become reliant on it is to be proved correct.

[217] '5th Generation' aircraft represent the culmination of a century of development and are defined by their significant advancements in information systems and associated software. For depth on the generations of aircraft, see:
Writer, "Five Generations of Jets ".
Gady, "China's First Fifth Generation Fighter Jet Is Operations".

[218] Taking the F-35 as an example, Lockheed-Martin claim technological enhancements achieved through harnessing of the cyber domain allow it to combine speed, agility, fully fused sensor information and network-enabled operations.
LockheedMartin, "About the F-35: The Multi-Variant, Multirole 5th Generation Fighter".
Norman, "Can the Us Military's New Jet Fighter Be Hacked?."
Roblin, "Can China's Chengdu J-20 Stealth Fighter Win against America's F-35 or F-22".

[219] E.J. Wilson, "Hard Power, Soft Power, Smart Power", *The Annals of the American Academy of Political and Social Science,* 616 (2008): 110.

[220] UK, "Joint Defence Doctrine 0-01 Uk Defence Doctrine", 1.

Soft Power

In exploring this, the first alternative to examine is soft power. Defined as the art of 'getting others to want the outcomes that you want' through co-option rather than coercion, soft power has become an important activity for all states[221]. Often associated with intangible concepts including culture and values, it does not offer as clear an example of influence as hard power because, by its nature, soft power is 'intangible…and inherently difficult to quantify'[222]. Given this, the inclusion of the military in soft power could be argued to blur the line of strategic effect to a point at which the lever has no value.

This assertion has unsurprisingly elicited debate. For example, from one definitional perspective soft power excludes any involvement of the military lever as the concepts influence is only 'achieved through activities which are not formally organised by Governments'[223]. However, as the UK Parliamentary Select Committee on Soft Power argues, the concept 'is not divorced from governments' as all the levers of national power can make a state more attractive to others[224].

A position supported by Pamment, he argues that in the 21st century soft power has emerged to represent the integration of, amongst other factors, diplomacy, aid culture and security. This is linked by Pamment to contemporary Western conceptualisations of soft power which he characterises as 'essentially theories of winning globalisation by generating desired outcomes'[225]. Whilst Gray counters such assertions by arguing that an ill balanced focus on the military's involvement in soft power creates a paradox that it works well when not needed but becomes irrelevant in a crisis, a picture nonetheless emerges on the relevance of the military in soft power[226].

[221] Nye, "Public Diplomacy and Soft Power", 95.
[222] McClory, "The New Persuaders: An International Ranking of Soft Power", 1.
[223] Museum Directors Council, "Soft Power ", (2019).
[224] UK, "Persuasion and Power in the Modern World - Select Committee on Soft Power and the Uk's Influence", ed. Select Committee on Soft Power (2014), 35.
[225] J. Pamment, *British Public Diplomacy and Soft Power: Diplomatic Influence and the Digital Revolution* (London: Springer, 2016), 239.
[226] C.S. Gray, *Hard Power and Soft Power: The Utility of Military Force as an Instrument of Policy in the 21st Century* (Pennsylvania: US Army War College, 2011), 53.

Explored by Machain in his reflection on 'a small but growing' body of academic literature which focuses on the value of 'military soft power', the argument is acknowledged by official sources [227]. Including the aforementioned UK Parliamentary Select Committee, it embraces the use of military capabilities for soft power effects in the right circumstances[228]. This argument therefore leads one to conclude that this concept may not offer as clear an example of influence as military hard power but is, nonetheless, impactful[229].

This argument appears to contradict the realist assertions that underpin this thesis' proposal. However, as Nye further contends, realists 'who deny the importance of soft power are like people who do not understand the power of seduction'[230]. Continuing the argument, he suggests that just because you cannot drop a thing 'on a city or on your foot' does not mean that thing lacks power[231].

An argument embraced by states, military capabilities have routinely been employed to deliver soft power. For example, Keck lists numerous examples ranging from Allied personnel in Japan and Germany assisting in post-war transformations, through to humanitarian support following natural disasters[232]. Though incorporating all elements of the military from soldiers delivering aid to sailors assisting in disaster recovery, air power's soft power role has a long and distinguished history.

Discussed by Lowther in terms of 'air diplomacy', three distinct areas of utility are identified which, being unique to air power, allow it to outperform land and maritime forces in the soft power role[233]. The first of these, humanitarian support,

[227] For Machain, see:
C.M. Machain, "Exporting Influence: U.S. Military Training as Soft Power", *Journal of Conflict Resolution* 65, no. 2-3 (2020).
Other examples of the 'small but growing' body of academic literature signposted by Machain include:
Atkinson, *Military Soft Power: Public Diplomacy through Military Educational Exchanges*.
M.A. Allen et al., "Outside the Wire: Us Military Deployments and Public Opinion in Host States", *American Political Science Review,* 114, no. 2 (2020).
[228] For the UK Parliamentary Select Committee report, see:
UK, "Persuasion and Power in the Modern World - Select Committee on Soft Power and the Uk's Influence".
[229] Clinton, "Transcript of Clinton's Confirmation Hearing to the Senate Foreign Relations Committee".
[230] Nye, "Public Diplomacy and Soft Power", 95.
[231] Ibid.
[232] Z. Keck, "The Hard Side of Soft Power", *The Diplomat*, 24 July 2013.
[233] Lowther, "Air Diplomacy: Protecting American National Interests", 4.

is the most intuitive. Beginning with the Berlin airlift from 1948 to 1949, states have frequently used air power to deliver humanitarian support. A contemporary example of this is the US Air Force delivering aid to Beirut in 2020 following a major explosion in the port[234].

Apparently clear, some have questioned whether the state motivation behind such activity is truly ever 'soft'. Taking Berlin as an example, the events have been characterised as the final Soviet step in an 'orchestrated campaign of graduated pressure'[235]. In this narrative, the Soviets were countered by the hard power of Allied air forces breaking the blockade and defeating coercion at any cost. Whilst having credence and indicating that in part the airlift is an example of hard power, a more convincing argument is offered by Lowther who concludes that whilst hard power aspects exist, the use of air power to deliver humanitarian aid elicits soft power through 'goodwill with governments and citizens around the globe'[236].

When considered in relation to the Berlin airlift, the event can be viewed as embodying this mixed context. Notably, though an initial hard power motivation may have driven the Allied action, the grateful reaction of Berliners to keep them alive and the long-term result of 30 million American soldiers, their families and diplomats living in West Germany from 1945 to 1994 created a dominant soft power effect only possible because of air power[237]. Therefore, the role and importance of air power in humanitarian soft power becomes convincing.

Though such impact through the military lever is not unique to air power, what is unique is its speed, reach and versatility. When combined, these allow states to deliver humanitarian aid with air platforms more quickly, to more destinations and with less logistical support than through land or sea. Based on this, it is evident that with humanitarian aid being a staple of states soft power provision, and air

[234] For depth on the Berlin Airlift, see:
O'Connell, "'Uncle Wiggle Wings': Children, Chocolates and the Berlin Airlift".
For the Beirut example, see:
Venhuizen, "Air Force C-17s Delivering Relief to Beirut Following Deadly Explosions'".
[235] Harrington, "The Berlin Blockade Revisited", 99.
[236] Lowther, "Air Diplomacy: Protecting American National Interests", 4.
[237] The Associated Press, "Berlin Airlift: Germans Look Back and Forward", *NBC News* 2008.

power being the most versatile asset through which to deliver this, states are likely to become reliant on the capability.

Whilst this may represent the most obvious example of 'air diplomacy', Lowther's other areas also demonstrate air power's breadth. The first of these, public engagements, routinely take the form of air shows and displays of capabilities such as the UK Red Arrows 2016 tour of the PRC[238]. Building UK-Sino relations, positive engagement in this way has been used for over a century to achieve effective soft power results[239].

In the last, Lowther highlights the increasing trend for air forces to use their personnel's skills to train and develop other states[240]. Though not necessarily a use of air platforms, air power must be considered more than its constituent parts. With people intrinsic to its delivery, it is reasonable to consider, as Atkinson argues more broadly with reference to military exchanges, that the use of air force personnel to deliver soft power through training and interaction has soft power value[241].

With these soft power roles of 'air diplomacy' also recognised in military doctrine, it is evident that its value figures in a state's calculation on power and influence[242]. Admittedly often intangible and focused on air power as an enduring rather than a technologically advanced capability, the advantages are not only longer lasting than hard power but more cost-effective. A significant consideration in a climate of austerity, 'air diplomacy' allows air forces to deploy aircraft for specific soft power taskings across all the categories without the overheads of land and sea[243]. Given this, we begin to build a picture of depth in the utility air power

[238] BBC, "Red Arrows Touch Down in China on World Tour".
[239] For example, Lowther highlight's that the US Army Aviation Section sent a 'small fleet of aircraft on a successful cross-country tour in 1910, eventually leading to widespread support for military aviation'.
Lowther, "Air Diplomacy: Protecting American National Interests", 4.
[240] Ibid.
[241] Atkinson, *Military Soft Power: Public Diplomacy through Military Educational Exchanges*.
[242] For an example of military doctrine on air power's role in soft power, see:
UK, "Joint Doctrine Publication 0-30: Uk Air and Space Power, 2nd Ed", ed. Concepts and Doctrine Centre (Great Britain Ministry of Defence Defence, 2017), 2.
[243] Arguments for the cost effectiveness and flexibility of air power in soft power are made by:
Lowther, "Air Diplomacy: Protecting American National Interests".

offers. Taken collectively, a pressing argument as to why states are likely to become reliant on air power is brought into focus.

Smart Power

Whilst the above discussion indicates that air power is central to a state's hard and soft power, the last point to explore is its distinctive utility for smart power. A term coined by Nye in his argument that soft power alone cannot produce effective foreign policy[244], the concept was popularised in 2009 by US Secretary of State Hillary Clinton. Using it in her address to the Senate Foreign Relations Committee, she argued that the US cannot solve the world's problems alone but, equally, the world cannot solve them without the US. The solution, she suggested, is to employ 'smart power, the full range of tools at our disposal'[245].

Taken in simple terms, this interpretation of smart power is the capacity to combine hard and soft power in a mutually reinforcing manner[246]. Though this requires the artful combination of 'conceptual, institutional, and political elements' from across all instruments of power[247], it is undeniable that the military instrument plays a central role. A fact which continues to be enhanced as the information age develops, Nye himself recognised that military success is no longer 'whose army wins but…whose story wins'[248].

With recognitions of its utility growing since the end of the Cold War[249], smart power has been applied by various militaries in their legitimisation of interventions

[244] Nye, "Combining Hard and Soft Power", 161.
[245] Clinton, "Transcript of Clinton's Confirmation Hearing to the Senate Foreign Relations Committee".
[246] Wilson, "Hard Power, Soft Power, Smart Power", 115.
[247] Ibid.
[248] Nye, "Combining Hard and Soft Power", 162.
[249] An example of this post-Cold War growth of smart power manifesting is the concept of R2P, a development of the Lockean inspired concept of 'just war'. For depth on R2P and 'just war' theory, see:
Crawford, "Just War Theory and the Us Counter Terror War", 7.
Augustine, *The City of Gods: Against the Pagans* 161.
Annan, "Secretary-General's Annual Report to the Un General Assembly ".
Annan, "We the Peoples: The Role of the United Nations in the 21st Century ".
Evans and Sahnoun, *International Commission on Intervention and State Sovereignty (Iciss), the Responsibility to Protect*
UN, "2005 World Summit Outcome Document ".

and subsequent attempts at nation building[250]. Reflecting on the role air power has played in these activities it is evident that when its soft and hard power roles are combined air power must also be central to smart power. With smart power also likely to be a continued refrain in the strategies of states, it adds depth to the argument of why states are likely to procure, and become reliant on, air power.

Strategic Objectives and the Utility of Air Power

The above discussion on the instruments of power, and its manifestation as hard, soft, and smart, provides an insight into how air power must be considered pivotal in translating realist-constructivist motivations into deliverable means. However, to confirm the arguments validity, and underline this thesis' proposition for the 'first cause' of air power's cyber risk, we must delve further. To do so, it is necessary to examine how the motivation for power is in practice translated into influence under the guiding hand of strategy and, within this, the importance air power plays.

Strategic Objectives

To begin this discussion, we must first understand the concept of strategy and how it is expressed through strategic objectives. Providing a thoughtful opening, Porter reminds us that strategy is 'the orchestration of ends, ways, and means'[251]. This, he goes on to explain, is a balancing act in which resources are weighed against commitments and interests so that power may be translated into political ends at a cost that is acceptable to the state[252]. Though manifested across all instruments of power, it is for the reasons of pre-eminence discussed above that the military instrument remains central to this process.

[250] For example, the Coalitions interventions in Iraq and Afghanistan saw hard power in the form of military force combined with nation building and palliative support in the form of humanitarian aid. Though the end results of these interventions can be debated, the use of smart power in their delivery is clear.
A. Chong, "Smart Power and Military Force: An Introduction", *Journal of Strategic Studies,* 38, no. 3 (2015): 234.

[251] P. Porter, "Why Britain Doesn't Do Grand Strategy", *The RUSI Journal,* 155, no. 4 (2010): 6.

[252] Ibid.

Exploring this importance, Betts reaffirms the role of military strategy as the link 'between military means and political ends'[253]. Expressed by states through publicly available strategy documents, the aim is to set parameters which will focus the military instrument so that ends are achieved, and military power does not become 'a loose cannon'[254]. Remaining high level, these documents are routinely arranged into themes which set the direction of travel for military practitioners.

An analysis of strategies published by a range of states confirms commonalities within this adoption of themes. Whether expressed as 'pillars' by the US, 'interests' by France, 'objectives' by Australia or under a broader 'framework' which in turn establishes objectives by the UK, what all share is a distillation of political intent into a small number of definable categories. These, when achieved through the military instrument, are intended to assure a states realist desire to survive and, above this, the constructivist intent to maintain roles and status[255].

Given the bracketed nature of these objectives, they can be viewed as offering an identifiable and analysable baseline from which to assess whether air power has become indispensable to achieving influence. In making this statement, however, it is recognised that such objectives generated by Governments for the purpose of public consumption can, due to the nature of political rhetoric, be considered as glossing over internal contradictions. As a result, their use for academic analysis within this thesis might be considered flawed.

For example, whether phrased as 'pillars', 'interests' or 'objectives', many national strategies employ the terms 'protect' and 'project' as structural signposts. Though neatly definable, these can from an academic perspective be fraught with contradictions. Illustrated through the scenario of a terrorist-attack, one could conceive a situation in which the 'projection' of influence forms the motivation for

[253] Betts, "Is Strategy an Illusion?", 5.
[254] Ibid.
[255] Examples of National Security Strategies include:
US, "National Security Strategy of the United States of America".
UK, "Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy".
Australia, "Strong and Secure: A Strategy for Australia's National Security".
Republique-Française, "Defence and National Security Review: Strategic Review ".

an attack that ultimately jeopardises the 'protection' of national security. With this demonstrating how objectives even when apparently distinct are not only entwined but potentially contradictory, it could be concluded that their use for academic analysis is inadvisable.

Whilst acknowledged, this assertion can be countered by the argument that to understand the nature, strength, weaknesses, and potential impact of national strategies it is necessary to evaluate them through the lenses in which they are encased. Therefore, in exploring whether states have become reliant on air power it is necessary to consider the strategies in their own vernacular. Based on this, and a review of how strategies have been expressed, this thesis will for the remainder of the Chapter focus on three common themes: protecting national sovereignty, projecting global power, and promoting national prosperity[256].

Protecting National Sovereignty

Considering the first, the protection of national sovereignty, the aim is expressed succinctly by the UK which defines it as the intent to protect 'territory, economic security, infrastructure and way of life'[257]. An aspiration common to all independent states, it is essential for not only survival but also the maintenance of role and status. This is because if a state cannot protect its own sovereignty, it will, in a worst-case scenario, be destroyed. Alternatively, even if destruction can be prevented, a state unable to assure the sanctity of its sovereignty is in the constructivist sense unlikely to maintain the role to which it aspires.

[256] Though these are taken from the UK strategy, they closely align to the Australian objectives of 'protect, secure and promote' and the US pillars 'protect, promote, preserve and advance'.
US, "National Security Strategy of the United States of America".
Republique-Française, "Defence and National Security Review: Strategic Review ".
UK, "National Security Strategy and Strategic Defence and Security Review: A Secure and Prosperous United Kingdom", ed. HM Government (Great Britain HM Government, 2015).
Australia, "Strong and Secure: A Strategy for Australia's National Security".

[257] UK, "National Security Strategy and Strategic Defence and Security Review: A Secure and Prosperous United Kingdom".

Aerial Sovereignty

To address how the political aims of this protectionist theme can be achieved by the military instrument, it is first necessary to remind ourselves of what must be protected. To do so we should return briefly to the Westphalian state-centric ideals of sovereignty which have endured into the 21st century. Despite being challenged by 'post Westphalian' issues, the principles established in 1648 continue to define national boundaries.

Considering this further, the concept of territorial sovereignty was until the 20th century a two-dimensional issue revolving around land and sea borders. To protect their sovereignty, nations were only required to prevent the crossing of land borders and agreed areas of nationally controlled water [258]. Though admittedly not an easy task, its two-dimensional nature and the limited speed of land and sea movement allowed risks to be mitigated.

With the advent of powered flight in the 20th century the challenges of securing state sovereignty increased. First, with air platforms able to rise above traditional borders, states were forced to shift to a three-dimensional concept of sovereignty[259]. Second, with air power increasing in speed and reach, states were also forced to confront the issue of aerial sovereignty being compromised with little or no warning. Finally, when such compromise was achieved, states had to manage the distinctive physical and psychological effects that air power can deliver before the offensive capability retreats to safety[260].

Taken in combination, air power offered states a uniquely effective means of undermining sovereignty. Though its first use by Germany in 1918 would not be

[258] Land borders are under Westphalian principles broadly understood. The line of sovereignty for costal states has been subject to more debate. For the contemporary interpretation of maritime sovereignty, see:
UN, "Oceans and Law of the Sea. The United Nations Convention on the Law of the Sea", (1988).

[259] This concept of a third dimension in national sovereignty has been a point of considerable debate since the invention of powered flight. Solutions have however been offered in Article I of the 1919 Paris Convention for the Regulation of Aerial Navigation which was replaced in 1944 by the Chicago Convention on International Civil Aviation. Other key developments include the creation of the International Civil Aviation Organisation (ICAO).
Banner, *Who Owns the Sky? The Struggle to Control Airspace from the Wright Brothers On* 42.
ParisConvention, "Convention for the Regulation of Aerial Navigation", 195.
Williams, "A Crisis in Aerial Sovereignty? Considering the Implications of Event Military Violations of National Airspace", 51.

[260] "A Crisis in Aerial Sovereignty? Considering the Implications of Event Military Violations of National Airspace", 15.

decisive, the events acted to highlight the dangers of the 'third-dimension'[261]. Developing in line with air power's rise to become a preeminent capability, this threat had by the Second World War's use of strategic bombing eclipsed land and sea borders as a state's greatest single point of vulnerability in the initiation and progression of conflict. By this logic, to assure survival, role, and status through the protectionist objective, states must first and foremost be able to control their own aerial sovereignty[262].

Having understood the space which states must now protect and the challenges this entails, the next point to establish is how seriously states have taken the requirement. A principal factor which illustrates this are airborne nuclear capabilities. Responding to the unrivalled destructive force the US delivered via air power in 1945 to end the war in the Pacific, the world recognised how the ability to compromise aerial sovereignty and deliver nuclear weapons offered the ultimate expression of hard power[263]. Creating the basis for deterrence strategy, the seriousness the US placed on being able to compromise aerial sovereignty, and deter the compromise of its own sovereignty, was shown by its maintenance until 1991 of a strategic airborne nuclear capability at permanent readiness[264].

Beyond this extreme example, states experience of and response to conventional warfare has also proven why assuring aerial sovereignty is key to the protectionist objective. Whether referring to the routine projection of air power into the skies above others who are unable to prevent it[265], or the pre-emptive projection of air

[261] This refers to the German use of Zeppelin Airships to attack Britain on 19-20 January 1915.
Stephenson, *Zeppelins: German Airships 1900?* , 13.

[262] Early discussions on the importance of assuring national aerial sovereignty in the post-war period were made by:
O.J. Lissitzyn, "The Treatment of Aerial Intruders in Recent Practice and International Law", *The American Journal of International Law,* 47, no. 4 (1953): 559.
Further cotemporary discussion is offered by:
Williams, "A Crisis in Aerial Sovereignty? Considering the Implications of Event Military Violations of National Airspace", 52.

[263] This refers to the dropping of atomic bombs on Hiroshima and Nagasaki in 1945 forcing the surrender of Japan.
BBC, "Hiroshima Bomb: Japan Marks 75 Years since Nuclear Attack", 2020.

[264] The US, for example, maintained nuclear armed bomber on 24/7 ready alert until the end of the Cold War in 1991.
M. Weisgerber, "Us Preparing to Put Nuclear Bombers Back on 24-Hour Aler", *Defence One*, 22 October 2017.

[265] For example, from 2002 the US has used air power in the form of UAVs flown from regional locations but often piloted from the mainland US to pursue their national interests in states including Pakistan, Yemen and Somalia. Alternatively, on a more regional basis, Chinese military aircraft since 2019 have been reported to have entered Taiwanese airspace as part of the long running debate over Taiwanese sovereignty on an 'almost a daily' basis as they attempt to extend their influence in the South China Sea.
A. Plaw, M. S. Fricker, and C. R. Colon, *The Drone Debate: A Primer on the Us Use of Unmanned Aircraft Outside Conventional Battlefields* (London: Rowman and Littlefield, 2015), 1.

power which has been decisive in the outcome of major conflicts[266], the ability to protect aerial sovereignty from conventional threats has become a defining feature of military success in the 20th and 21st centuries.

Reflecting on the other arguments presented above, it can be concluded that in considering the protectionist objective, assuring aerial sovereignty must be considered first and foremost. Though land and sea sovereignty remain important, they are secondary in contemporary conflict. This is underlined by Montgomery's assertion that 'if we lose the war in the air, we lose the whole war and lose it quickly'[267].

If one is to accept this argument: the next question is what capabilities states require to translate the political aim into military means? Though in answering this Ground Based Air Defence (GBAD) assets from radars to missiles remain important, the principal capability will always be air platforms. Of these, the highest profile and most relied on are the advanced fighter aircraft which can respond to immediate threats.

Referred to in their national protectionist role as either Quick Reaction Alert (QRA) or Airspace Control Alert (ACA) depending on the nation, this military task designed to assure aerial sovereignty has a long history[268]. First featuring in the Second World War, QRAs were manned by British Royal Air Force (RAF) pilots operating advanced Spitfire and Hurricane aircraft. Held at readiness throughout the Battle of Britain in 1940 to intercept the German Luftwaffe, their successful protection of aerial sovereignty offers a clear example of how its defence can prevent the destruction of a nation[269].

B. Blanchard and Y. Lee, "Chinese Fighter Jets Enter Taiwan Airspace in 'Threat to Regional Peace", *Independent*, 9 September 2020.

[266] For example, the decisive nature of the use of pre-emptive air power in subsequent conflicts are numerous. Two of the most prominent examples include the Israeli Air Forces (IAF) 1967 near destruction of the Egyptian, Jordanian, Iraqi and Syrian Air Forces in the 6 Day War and the US led Coalitions 'Shock and Awe' campaign in the 1991 Gulf War.
S. Dunstan, *The Six Day War 1967: Sinai* (London: Bloomsbury, 2012), 39.
H. Ullman, "War in Iraq: Shock and Awe Revisited", *The RUSI Journal,* 148, no. 3 (2003).

[267] Montgomery, "The Role of Science in Warfare of the Future".

[268] QRA is used by Britain and most NATO countries. ACA is preferred by the US.

[269] UK, "Battle of Britain ", ed. Royal Air Force (Great Britain 2020).
N. Rees, "Raf's Quick Reaction Alert Reveale", *News Story*, 20 September 2012.

Though such stark examples of national survival are thankfully no longer as common, the events of 11 September 2001 (9/11) reinvigorated awareness of QRAs and the defence of aerial sovereignty. In the US for example, the reaction to 9/11 resulted in its QRA provision being enhanced. Leading to an increased capability, the North American Aerospace Defense Command (NORAD) 'scrambled' its QRA to meet over 64,000 reported threats between 2001 and 2014[270].

Becoming synonymous as a 'nation's only guardian against a diverse array of airborne threats'[271], the importance of the QRA is only matched by the importance of aerial sovereignty itself. Though a fact which is respected by all states, it is perhaps most acutely felt by those with both aggressive neighbours and an inability to achieve the protectionist objective through domestic means.

Situations meeting these criteria are numerous. For example, Taiwan has reported 'almost daily' contraventions of its aerial sovereignty by the PRC since 2019 and, despite a capable air force, relies on the deterrence of its alliance with the US to assure the protectionist objective[272].

A further example is within the Baltic states. With both the states themselves and their North Atlantic Treaty Organisation (NATO) allies considering Russia to present a credible threat to not only aerial sovereignty but their national survival, a NATO QRA under the banner of Baltic Air Policing was established in 2004. Reinforced in 2014 after the Russian annexation of Crimea, this long running commitment proves the value placed on defending aerial sovereignty. Furthermore, it also reinforces the fact that the Baltic states view NATO's hard power, as expressed through air power, to be more effective than the European Union's (EU) soft power when translating the protectionist objective into meaningful influence[273].

[270] For depth on NORAD and Operation Nobel Eagle, see:
C.R. Davis, "Presentation to the Senate Armed Services Committee: Subcommittee on Tactical Air and Land Force", ed. Senate Armed Services Committee (2014), 6.

[271] D. Kang, "Guardians of the Homeland: Looming Threats to the Air Alert Mission", *War on the Rocks*, 6 June 2016.

[272] Blanchard and Lee, "Chinese Fighter Jets Enter Taiwan Airspace in 'Threat to Regional Peace".

[273] For an example of Russia's frequent contraventions of sovereign air space which necessitates the NATO QRA, see:

In considering the above examples, we are presented with a clear conclusion. Specifically, if states are to both survive and maintain their role and status, they must be able to protect their aerial sovereignty or be part of a coalition that can do so for them. With air platforms the primary means to achieve this, states must procure air power to thrive and survive. Once they have done so, they will become reliant on this air power if they hope to continue to achieve the strategic objective.

Land and Maritime Sovereignty

To reinforce this point, it is instructive to also consider air power in its wider protectionist role. For example, a second essential capability offered by air power is found in the sphere of airborne Intelligence, Surveillance and Reconnaissance (ISR) and its impact on states ability to secure their land and maritime borders.

Originally developed for military use, airborne ISR has evolved from air balloons observing enemy troop movements, through aerial photography to modern UAVs with long loiter times and digital links[274]. Increasingly capable, it has become indispensable to military decision-makers. Though remaining essential on the battlefield, it has also in the last two decades begun to transition into, and become pivotal for, the protection of national sovereignty through oversight of land and maritime borders[275].

Considering first land borders, Marin reflects that 'once upon a time' land borders were defined by border points where guards would check passports[276]. However,

NATO, "Russian Fighter Jet Violated Nato Airspace over Bornholm Island'", ed. NATO Newsroom (2020).
For detail on Baltic Air Policing, see:
"Baltic Air Policing ", ed. NATO Newsroom (2020).
For detail on the Baltic state's preference for the military hard power of the QRA, see:
C. Matteo, "How and to What Extent Do the Baltic States Feel Geopolitically Threatened", *Journal of Diplomacy and International Relations,* 16, no. 2 (2015): 79.

[274] For detail on the development and use of airborne ISR in a military environment, see:
M. Alderton, "Airborne Isr", *Trajectory Magazine*, 4 December 2013.
NATO, "Joint Intelligence, Surveillance and Reconnaissance", ed. NATO Newsroom (2018).
P. C. Nolin, "Unmanned Aerial Vehicles: Opportunities and Challenges for the Alliance'", *NATO International Secretariat Special Report,* (2012).

[275] R.E. Moutray and A.M. Ponsford, "Integrated Maritime Surveillance: Protecting National Sovereignty', " in *International Conference on Rada* (2003), 2.

[276] L. Marin, "Is Europe Turning into a 'Technological Fortress'? Innovation and Technology for the Management of Eu's External Borders: Reflections on Frontex and Eurosur," in *Regulating Technological Innovation* ed. M. A. Heldeweg and E. Kica (London: Palgrave McMillan), 132.

with an increase in transnational concerns from global migration to terrorism and criminality being securitised, the pressure on states to think wider and not accept limited control has become overwhelming[277].

In response, organisations including FRONTEX, the EU's Border and Coast Guard Agency, have readjusted their approach toward an increased use of UAVs. Viewed as cost-effective and versatile, their employment to deliver airborne ISR has increased the EU's confidence that it is able to protect its collective national sovereignty from transnational threats[278].

Though Csernatoni argues that this use of high-end technology is not the panacea some might hope, states' use of air power to achieve the protectionist objective in this context is not limited to the EU[279]. With other examples including the US Department of Homeland Security (DHS) increasingly investing in 'airborne sensors', there is no doubt that the cost-effective solution of airborne ISR will be a staple of securing land borders[280].

This trend is also increasingly prevalent in the maritime environment. Leading to the concept of Integrated Maritime Surveillance (IMS), advanced manned and unmanned airborne ISR platforms are combining to form 'families of systems'[281]. Through this approach coastal nations are now able to protect large areas of open water with air platforms in a continuous, affordable, and real-time manner[282]. Balancing the trend of reducing naval capacities which would otherwise have placed maritime sovereignty at risk, this is, in the same vein as land borders, likely

[277] The concept of securitisation developed from the Copenhagen Schools 'widening' of the security agenda to include non-military issues such as migration and the environment. For depth, see:

Buzan, Wæver, and de Wilde, *Security: A New Framework for Analysis*
T. Baizacq, *Understanding Securitisation Theory* (London: Routledge, 2011), 60.
Eroukhmanoff, "Securitisation Theory," 105.

[278] R. Csernatoni, "Constructing the Eu's High-Tech Borders: Frontex and Dual-Use Drones for Border Management", *European Security,* 27, no. 2 (2018): 176.

[279] Ibid., 177.

[280] For further detail on US DHS use of airborne sensors, see:

US, "Air Based Technologies", ed. DHS Science and Technology Directorate (Department of Homeland Security 2017).

[281] For example, the US intent is to combine the surveillance capabilities of the Boeing Poseidon P8 Maritime Patrol Aircraft (MPA) with the long loiter time of the Triton UAV to achieve unparalleled maritime coverage in securing its sea borders.

B. Baker, "Us Navy's Triton Uas – Poseidon's Perfect Partner", *Naval Technology*, 9 November 2014.
W.A. Perkins, "Enabling Maritime Isr through the 'Family of Systems'", *The Journal of the Joint Air Power Competence Centre,* July (2017): 15.

[282] Moutray and Ponsford, "Integrated Maritime Surveillance: Protecting National Sovereignty', " 2.

to be an enduring means of transferring political intent into meaningful influence[283].

Reflecting on the above discussion it is evident that the protectionist objective of national strategies is felt most acutely in aerial sovereignty. This is because if states are to both survive and maintain their role and status against credible state threats, this aspect of sovereignty must be defended. Within this, the role of air power in providing QRAs was shown to be the central means of translating the political objective into effective military means. For this reason, states are highly likely to continue to acquire, and thereafter become reliant on, air power.

Turning finally to the pressures of land and maritime borders, this area which focuses on transnational threats does not necessarily pose an existential issue. However, increasingly securitised, states are against a backdrop of austerity seeking cost-effective technological means of protecting long land and maritime borders. With a solution to the protectionist objective in this area being offered by airborne ISR, it is again likely that states will continue the trend of acquiring and becoming reliant on air power.

Projecting Global Power

Having shown that air power is the cornerstone of the protectionist objective, it is next necessary to consider the second theme of projecting global power. Summarised by the UK, the political aim is to 'reduce the likelihood of threats materialising' and affecting the interests of not only the state, but its allies and partners[284].

[283] The UK provides an example of a maritime nation which is reducing its naval capability and is choosing to invest in airborne ISR as an alternate means of protecting its maritime sovereignty. For depth and discussion, see:

UK, "Sdsr 2015: Defence Fact Sheets, Defence Strategy and Priorities", ed. HM Government (Great Britain Ministry of Defence 2016).

Moutray and Ponsford, "Integrated Maritime Surveillance: Protecting National Sovereignty', " 2.

D. Nicholls, "Has the Royal Navy Got Enough Ships?", *The Telegraph*, 24 January 2020.

[284] UK, "National Security Strategy and Strategic Defence and Security Review: A Secure and Prosperous United Kingdom", 11.

To translate this into military means, Matlary suggests that states have four key options: deterrence, coercion, containment, and confrontation[285]. Discussing these further, he notes that they are not mutually exclusive. For example, the combination of deterrence and containment became the basis of Western strategy during the Cold War[286]. Given this, for the purpose of this discussion, the project objective will be narrowed to its two core components: deterrence and coercion.

Deterrence

Considering first deterrence, this concept grew at speed during the Cold War to become a highly influential theory[287]. Derived from the Latin 'terrere' meaning to terrify, it is intuitively linked with the intent of terrorists to achieve political ends through the threat of horrific attacks. However, in the global sense, when adopted by states, it has come to be more closely associated with the deterrent effect of nuclear weapons[288].

Dominating post-war academic thinking, deterrence theory would also seep into broader Western intellectual thought and military policy[289]. Driven by an attractiveness of its 'clearheaded logic, which is as persuasive as it is elegant', the concepts which underpin deterrence have informed conventional military strategy[290]. Specifically, states have increasingly used it to justify large conventional capabilities which can be held at a high readiness near to an adversary. Used to signal a potential aggressor, the common understanding is that fear of the consequences will prevent an attack from occurring[291].

Though logical, in his discussion of classical deterrence theory Paul highlights that the proposition only works if three core premises are met: a deterrer must

[285] Matlary J.H., *Hard Power in Hard Times* (London: Palgrave Macmillan, 2018), 11.
[286] Ibid.
[287] C. H. Achen and D. Snidal, "Rational Deterrence Theory and Comparative Case Studies", *World Politics,* 41, no. 2 (1989): 143.
[288] S.W. Oam, "Nuclear Deterrence Theory-a Threat to Inflict Terror", *Flinders Law Journal,* 15 (2013): 258.
[289] Achen and Snidal, "Rational Deterrence Theory and Comparative Case Studies", 143.
[290] Ibid., 258.
[291] R.J. Overy, "Air Power and the Origins of Deterrence Theory before 1939", *The Journal of Strategic Studies,* 15, no. 1 (1992): 73.

have sufficient capability, the threat of using that capability must be credible, and both preceding factors must be clearly communicated. With Paul pointing out that these elements must 'operate across all classifications of deterrence', the key question for states is that if deterrence is to be used, what military 'means' are best to do so?[292]

As touched on above, the highest-profile example of a military deterrence is the nuclear capability. Based on the premise that nuclear weapons would 'inflict suffering and destruction so horrific that…no leader would risk it by attacking a nuclear-armed state', this approach was the mainstay of the US and Soviet Cold War policies[293].

Beyond this overarching logic, a second key concept is the second-strike capability. Based on the assertion that to have a credible deterrent a state must be able to absorb a nuclear first strike and then retaliate, states were forced to identify ways of maintaining secure second-strike forces. Though air power would play a key role in this during the Cold War, it has largely been replaced in the post-Cold War period by Intercontinental Ballistic Missiles (ICBM) and Submarine Launched Ballistic Missiles (SLBM)[294].

Given this, it is evident that whilst air power has been a mainstay of deterrence for nuclear armed states, this reliance has waned. Though this might suggest that in the 21st century air power is not a core means of deterrence, the assumption would be wrong. This is because not only has the nuclear deterrent moved on, but the world has also moved on from the nuclear deterrent.

At the core of this shift is a fundamental criticism of the nuclear deterrent. As Powell argues, the assured-destruction capability provided to states offers the ability to ensure that 'the cost an adversary has to bear in any conflict outweighs

[292] T.V. Paul, *Complex Deterrence: Strategy in the Global Age* (Chicago University of Chicago Press, 2009), 2.
[293] Oam, "Nuclear Deterrence Theory-a Threat to Inflict Terror", 258.
[294] For a review of the use of air power in the Cold War, see:
M. Armitage and R. A. Mason, *Air Power in the Nuclear Age: 1945-84* (London: MacMillan), 1985).
For a discussion on second strike capabilities including the current focus on ICBMs and SLBMs, see:
A. Long and B.R. Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy", *Journal of Strategic Studies,* 38, no. 1 (2015).

any possible gains'[295]. Therefore, faced with a nuclear armed adversary, the logic dictates that the aggressor will always back down. However, following the advent of second-strike capabilities, a state also knows that if it were to use its nuclear arms the action would inevitably end in its own destruction. Given this, Powell concludes, the deterrent and second strike cancel each other out making the concept of a nuclear deterrence hollow[296].

Based on this, contemporary military means designed to fulfil the deterrent aspect of the project objective are conventional in nature. An increasingly accepted idea in the post-Cold War era, the point was underlined in 1997 by General Habiger, Commander in Chief of the US Strategic Command, when he commented that 'ultimately, deterrence is a package of capabilities, encompassing not just numbers or weapons, but an assured retaliatory capability provided by a diversified, dispersed, and survivable force'[297]. The question within this renewed perspective on deterrence is, therefore, what conventional military means have now replaced the nuclear deterrent?

To address this one must consider the varying types of threats states must deter in the 'post-Westphalia' era. Despite the rise in transnational actors, the most prominent remains other states. Within this, especially for super and great powers, the concern focuses on other great powers which can credibly threaten their national security.

It is noted that Morgan and Paul argue against this assertion, claiming that transnational issues have undermined the relevance of state-on-state conflict making this approach to deterrence no longer relevant[298]. However, events in the last decade show that Morgan and Paul's 2009 argument has become dated. For example, whether one refers to PRC expansionism in the South China Sea and

[295] R. Powell, "Nuclear Deterrence Theory, Nuclear Proliferation, and National Missile Defense", *International Security,* 27, no. 4 (2003): 89.
[296] Ibid.
[297] E. Habiger, "United States. United States Senate, Hearings before the Committee on Armed Services: Strategic Forces", ed. Committee on Armed Services (United States United States Senate, 1997), 182.
[298] P.M. Morgan and T.V. Paul, "Deterrence among Great Powers in an Era of Globalisation," in *Complex Deterrence: Strategy in the Global Age* ed. T.V. Paul (Chicago: University of Chicago Press, 2009), 260.

its border dispute with India[299], or Russia's actions against the Ukraine and an expansionist intent in the Baltic states and Eastern Mediterranean[300], great powers are increasingly showing a militaristic tendency. It is in countering these that conventional means of deterrence holds strong relevance to the project objective.

Those states seeking to achieve this deterrence must, therefore, identify what military 'means' offer the most credibility. In answering this with reference to NATO states and their deterrence of Russia, Veeble suggests that a combination of nuclear and conventional capabilities is necessary[301]. With this mirrored in other deterrent reliant areas such as the Eastern Mediterranean and East Asia, the issue is how sufficient conventional capability can be held in a region to achieve the aim.

Discussing the Baltics specifically, Veelbe goes on to comment that Russia had a clear conventional supremacy[302]. With Shlapak and Johnson underlining this in 2016 by highlighting that Russia could amass thirty to forty thousand soldiers in the region, it is hard to imagine how NATO, whose members are deterring on multiple fronts, could permanently match this conventional strength[303]. Though such figures have been diminished following Russian setbacks in Ukraine, regional political and military leaders in the Baltics continue to warn that Russia remains 'extremely dangerous'[304].

[299] The PRC has in the 21st century embarked on an increasingly aggressive expansionary strategy which includes the Belt and Road Initiative (BRI) and an assertive maritime policy in the South China Sea. For discussion on these, see:

J. Ball, "How Chinese Expansionism Fuels an Expansionist Foreign Policy", *Global Security Review*, 10 June 2019.

N. Jennings, "Deterring Chinese Aggression", *Small Wars Journal,* (2016).

[300] Litsas comments that since its annexation of Crimea and the long-term securing of Sevastopol for its Black Sea Fleet, Russia has continued to expand its influence in the area and the broader Eastern Mediterranean. For discussion on this, see:

V. Veebel, "Nato Options and Dilemmas for Deterring Russia in the Baltic States", *Defence Studies,* 18, no. 2 (2018): 235.

S.N. Litsas, "Russian in the Eastern Mediterranean: Intervention, Deterrence, Containment", *Digest of Middle East Studies,* 26, no. 1 (2017).

[301] Veebel, "Nato Options and Dilemmas for Deterring Russia in the Baltic States", 238.

[302] Ibid.

[303] D.A. Shlapak and M.W. Johnson, *Reinforcing Deterrence on Nato's Eastern Flank: Wargaming the Defense of the Baltics* (Santa Monica: RAND, 2016), 4.

[304] For quote, see:

Staff-Writer, "Russia Moved 80% of Troops from Nato Borders to Ukraine", *Rubryka*, 29 September 2022.

NATO's answer to achieving this deterrence has not been found in large land deployments but, rather, conventional air power used for deterrent purposes. Explored by Overy, this deployment of air power has, he suggests, become the 'central feature in the emergence of deterrence strategy'[305]. Developing through the strategic bombing of the Second World War to the Shock and Awe campaign of the Gulf War, it has been shown how air power with increasing precision is able to threaten both the national fabric and armed forces of an aggressor[306].

With such capabilities held at readiness to strike a potential aggressor regardless of their numerical superiority, one can appreciate why air power deterrence is effective. Summarising this argument as early as 1938, Charlton noted that air power is uniquely suited to this form of deterrence. Specifically, he stated that 'the very heart of a country now lies open to a peculiarly horrible form of attack which neither science nor invention can prevent, and to which no human skill or courage can be successfully opposed'[307].

Based on this logic, Western states have embraced the conventional use of air power by forward mounting it in relatively small but effective numbers to deter both Russia and China. Exploring this, Kainikara argues that if this use meets the three criteria of a credible deterrence, air power offers the most effective means of deterring state-based threats[308].

With the example of Baltic Air Policing providing evidence to this argument, it is concluded that conventional deterrence is necessary in the 21st century. With air power the most economic and credible means of delivering it, states who wish to achieve the project objective in the context of deterring other states have no choice other than to invest in, and become reliant on, the capability.

Having established the importance of air power in the context of state-on-state conflict, it is also necessary to turn toward a second issue in the 'post-Westphalia'

[305] Overy, "Air Power and the Origins of Deterrence Theory before 1939", 73.
[306] Ibid.
[307] L.E.O. Charlton, "The Menace of the Clouds", *The Aeronautical Journal,* 42, no. 327 (1928): 288.
[308] S. Kainikara, "The Strategy of Deterrence and Air Power", *Royal Australian Air Force, Air Power Development Centre* (2008): 7.

21st century: the transnational threat of violent non-state actors. Despite lacking the traditional power base enjoyed by states, these groups have shown an ability to project power and threaten states whose political values they oppose. Because of this, there is a requirement for states to themselves project power in the aim of deterring violent non-state actors.

In applying deterrence theory in this area, one must shift the concept towards a different perspective of asymmetric conflicts. Though deterrence in this context may seem implausible, Alder argues that from a constructivist perspective it makes logical sense. This is based on the assertion that as violent non-state actors are, like states, socially constructed entities they can also be made to fear destruction via military means[309].

An example of this in practice is Israel's deterrence of Hezbollah. Promising overwhelming military response to acts of aggression, Samaan's review of the conflict between 2006 and 2014 suggests that deterrence was successful. Specifically, an informal deterrence dialogue between Israel and Hezbollah led to an acceptance that the next round of fighting would be both devastating and likely to result in a perpetual cycle of retaliation. Based on their acceptance of this, Hezbollah was successfully deterred[310].

Critics of this use of deterrence argue, however, that the strategy may escalate rather than prevent violence. This is based on the premise that the acts of powerful states to deter may only inflame tensions in politically or ideologically motivated groups. Given this, attempting deterrence could be counter-productive[311].

However, alongside the Israeli example, others argue that not only does deterrence work in this scenario, but it is the deterrence offered by air power that is the most effective. Ideally suited to achieving the project objective in these

[309] Adler E, "Complex Deterrence in the Asymmetric-Warfare Era," in *Complex Deterrence* ed. T.V. Paul (Chicago: University of Chicago Press, 2009), 86.
[310] J. Samaan, "From War to Deterrence? Israel-Hezbollah Conflict since 2006", *Strategic Studies Institute, US Army War College* (2014).
[311] Adler E, "Complex Deterrence in the Asymmetric-Warfare Era," 86.

circumstances, states have since the late 1990s focused on the use of advanced UAVs for this purpose.

Though beginning in the Balkans in 1995 and Kosovo in 1999, Nolin notes that the turning point in the strategy of deterrence through UAVs was seen in the post-9/11 era[312]. Growing to be a critical element of the US led initiative to counter global terrorism, heavy investment had by 2012 seen the US UAV fleet grow to around 7,500 air platforms[313]. Quickly employed in every role from kinetic strikes to airborne ISR, it is the collective promise of their global projection against any assessed threats to the US without notice that forms the basis of the deterrent effect.

Exploring the mechanics of this further, commentators note that the West, led by the US, has drawn a 'red line' for any non-state group who might decide to plan, aid, or conduct attacks against Western nations[314]. If they do so, the US will use all means to identify, target and destroy, using armed UAVs, their leaders, fighters, and infrastructure. Though this has 'bent' international law through the contravention of third nation sovereignty[315], it has also established a position which clearly meets the three criteria of deterrence theory. Firstly, it has proven the capabilities of UAVs to achieve decisive effect. Secondly, it has underlined the credibility of the threat to use UAVs globally. Thirdly, through government statements and media coverage, the capability and its impact have been clearly and publicly articulated.

Critics of this position claim that despite the notable rise in the use of UAVs by the US, there has been no clear empirical evidence of its deterrence effect. Despite this, it remains a core aspect of Western deterrence strategy against

[312] Nolin, "Unmanned Aerial Vehicles: Opportunities and Challenges for the Alliance'", 5.

[313] Ibid.

[314] C. Chris, "Unmanned Deterrence: Deterring Terrorism with Armed Drones", SecBrief.org, https://www.secbrief.org/2013/05/unmanned-deterrence-deterring-terrorism-with-armed-drones/.

[315] For example, Article 2(4) of the UN Charter states that all Members must refrain from threatening or using force against other states. However, in their use of UAVs to strike targets in other Member states without their permission, the US has pointed to Article 51 that allows for an 'inherent right of individual or collective self-defence'. This 'bending' of international law allowed the US and its Western allies to act with freedom in contravening sovereignty if they can argue that those targets threaten their nation security.

UN, "Un Charter ", (1945).

L.E. Davis, M. McNerney, and M.D. Greenbery, *Clarifying the Rules for Targeting and Killing* (Santa Monica: RAND, 2016).

violent non-state actors[316]. Therefore, one can conclude that regardless of the evidence, it is an approach which states continue to trust and will therefore invest in. As such, deterrence of non-state actors through air power adds weight to the argument that states are likely to invest in, and become reliant on, air power.

Coercion

Having established the role of deterrence in the procurement and reliance on air power, the second area to consider in the project objective is coercion. In simple terms, coercion is the directing of instruments of power against an adversary to force them to stop their current actions. Though economic instruments are also used in this context, it is the military employment of hard power that endures as the most credible means of coercion[317].

Like deterrence, in that it aims to affect behaviour, coercion differs in the key aspect that it seeks to stop ongoing action rather than persuade an adversary not to initiate action. For this reason, coercion occurs in Pape’s view ‘whenever a state must choose between making concessions or suffering the consequences of continuing its present course of action’[318].

Though coercion has been a constant factor in mankind’s realist desire to survive, Byman et al comment that in recent years a certain style of coercion has, especially in the West, developed to reflect modern societal preferences. Relating to how and in what circumstances states are willing to threaten and use military force, they summarise this as being driven by five key characteristics[319].

Firstly, states have shown a preference to operate within coalitions so that the burden is shared, and their opponents are isolated from moral and material

[316] For media reports and studies underlining these points, see:
D. Kucinich, "Obama Administration Must Account to Congress for Targeted Assassination", *The Guardian*, 16 November 2012.
M.S. Akbar, "Obama or Romney: What It Means for a Pakistani Living under Drones", *CNN Political Op-Ed*, 6 November 2012.
PewResearchCentre, "Views on the Us and American Foreign Policy", in *Global Attitudes and Trends* (2012).
[317] J.H., *Hard Power in Hard Times*, 23.
[318] Pape, *Bombing to Win: Air Power and Coercion in War* 12.
[319] D. L. Byman, M. C. Waxman, and J. Shapiro, "The Future of Us Coercive Airpower," in *Strategic Appraisal: United States Air and Space Power in the 21st Century* ed. Z. Khalilzad and J. Shapiro (RAND: Santa Monica, 2002), 54.

support. Secondly, the public's intolerance for both their own military and foreign civilian casualties has narrowed the acceptable means through which coercion can be achieved[320]. Thirdly, this aversion to casualties has also been manifested in an aversion to seeing those considered 'innocents' enduring suffering because of coercive action[321]. Fourthly, the long-standing Western approach to conflict expressed in a 'reliance on materiel over manpower' has seen technological solutions increasingly replace low-technology mass when conducting coercive action[322]. Finally, though the West has continued to 'bend' legal interpretations, there has been a general drive to respect and adhere to the international rule of law[323].

In reflecting on the use of coercion within this 'new normal', a key question becomes which form of military capability is most suited to it? In answering this, one must recognise that in broad terms there are two main ways in which the military instrument can achieve coercive effect: punishment or denial[324].

In the first, punishment, the founding principle is to increase the costs or risks to the target state to a point at which they have no choice other than to capitulate[325]. Reflecting on this, Cohen argues above all other capabilities air power provides 'an unusually seductive' form of military means to achieve coercion through punishment[326].

This assertion was first made by Douhet. Discussed in his 1921 book *The Command of the Air,* Douhet contends that air power amongst all capabilities of the time, and any he could imagine in the future, was uniquely suited to coercion through punishment. Specifically, he argued that air power could force an

[320] Byman et al cite the US withdrawal from Somalia following the death of 18 US servicemen in 1993 as evidence of this 'strong pull that even low casualty levels can exert on US policy'.
Ibid., 56.

[321] Examples of this are evident in both the Vietnam conflict where concerns that civilian casualties would damage the US image at home constrained targeting choices and, more recently, in the 1991 Gulf War when the coalition air campaign took great lengths to avoid collateral damage in Iraqi population centres.
J. Olson, "The Effect of Civilian Casualties on Usaf Bombing Policy in Vietnam", *Air Power History,* 46, no. 44= (1999).
M. W. Lewis, "The Law of Aerial Bombardment in the 1991 Gulf War'", *The American Journal of International Law,* 97, no. 3: 485.

[322] Byman, Waxman, and Shapiro, "The Future of Us Coercive Airpower," 55.

[323] Ibid., 57.

[324] Pape, *Bombing to Win: Air Power and Coercion in War* 12.

[325] Ibid.

[326] E. A. Cohen, "Mystique of Us Air Power", *Foreign Affairs,* 73, no. 1 (1994): 109.

opponent through air-dropped high explosives or gas into a position in which they are 'living and working under constant threat…[and] oppressed by the nightmare of imminent destruction and death'[327]. Once achieved, this coercive effect would either force governments to concede or, if they would not, lead the population to revolt[328].

With other early air power theorists including Trenchard agreeing with Douhet's logic, Pape notes that punishment was the first coercive strategy fully embraced by air power practitioners[329]. Seeking to not necessarily affect an adversary's ability to resist, but the will to do so, the starkest examples can be found in the Allied strategic bombing campaigns of the Second World War[330]. Epitomised by the attack on Dreseden, Germany, in 1945 in which 135,000 civilians died, the Allies remained convinced that coercion by punishment delivered via air power would be decisive[331].

These war time claims would subsequently be supported by later official reports. For example, the US Strategic Bombing Survey (USSBS) published in 1945 concluded that though 'hindsight inevitably suggests that it might have been employed differently…Allied air power was decisive in the war in western Europe'[332]. Based on this, one might conclude that air power should be a key asset for states seeking to coerce opponents.

However, in moving the argument to the 21st century, and reflecting on Byman et al's 'new norms', the conclusion is undermined[333]. This is because whilst it is acknowledged that air power could deliver increasingly punishing strikes, it would not be palatable in most states for this to occur. This argument is supported by

[327] Douhet, *The Command of the Air*, 20.
[328] Pape, *Bombing to Win: Air Power and Coercion in War* 59.
[329] Ibid.
[330] K. Meuller, "The Essence of Coercive Air Power: A Primer for Military Strategists", *Air Power Review,* 4, no. 3 (2001): 49.
[331] M. E. Smith, "The Strategic Bombing Debate: The Second World War and Vietnam", *Journal of Contemporary History,* 12 (1977): 181.
[332] US, "The United States Strategic Bombing Survey: Summary Report", ed. United States Air Force (1945), 7.
[333] Byman, Waxman, and Shapiro, "The Future of Us Coercive Airpower," 54.

Conway-Lanz who concludes that the shift in 'transnational normative values' has since the Second World War precluded mass bombing of civilian targets[334].

Whilst this argument now precludes most states from adopting a strategy of coercion through punishment, it does not mean that coercion or air power as a tool to achieve it has lost its relevance. It is rather in the second form, coercion through denial, that contemporary focus now lies. Discussed in this context, coercion as a means of achieving the project objective focuses on employing military means to prevent adversaries from attaining political or territorial objectives. This is achieved by denying them the leadership, military or supporting capabilities to do so[335].

A more focused form of coercion, examples have been seen repeatedly in the post-Cold War period. Experienced alongside a move away from conventional warfare and a decline in the Clausewitzian concept of absolute war[336], this revised approach is now encased in expeditionary warfare and Counter-Insurgency (COIN) operations[337].

Taking expeditionary warfare as an example, this form of conflict can be defined as long-range operations without permanent basing[338]. Often seen to be used in combination with coercion through denial, a prominent and early post-Cold War example was the first Gulf War in 1990.

Discussing the Iraqi military strength before the conflict, Broader and Jehl identified that the state had the fifth largest army in the world with over a million personnel. Despite some critics identifying weaknesses including a dated air force and poor infantry tactics, it retained a core of veterans from the Iraq-Iran

[334] S. Conway-Lanz, "The Ethics of Bombing Civilians after World War Ii: The Persistence of Norms against Targeting Civilian in the Korean War", *The Asia-Pacific Journal,* 12, no. 37 (2014).
[335] Pape, *Bombing to Win: Air Power and Coercion in War* 12.
[336] The Clausewitzian concept of absolute war argued that the aim of warfare is to annihilate one's enemy. For Clausewitz's writing on this concept, see:

Clausewitz, *On War*

For arguments that Clausewitz's arguments on absolute war are no longer valid, see:

A. Wunische, "Reviewing Why America Loses Wars", *The Strategy Bridge*, no. October (2019).
[337] M. Gladius, "What Is an Expeditionary Force? No, Really, What Is It?", *Small Wars Journal,* (2020).
[338] Ibid.

conflict and had established fortified positions in Kuwait[339]. This made it a credible and dangerous opponent which was becoming increasingly aggressive in the Gulf Region.

Acting in response, the US led Coalition under Operation Desert Storm launched decisive military action to deter Iraqi aggression by denying it the ability to do so. Commencing in August 1990, this strategy would leave Saddam Hussein in power but reduce the 'Iraqi army to a smouldering wreckage in the desert' which was no longer able to threaten its neighbours[340].

Though this would be supported throughout the 1990s by economic sanctions, limited uses of coercion and weapons inspections, the fact of the subsequent Gulf conflict in 2003 might suggest that the strategy failed[341]. However, the use of coercion to deny did contain an aggressive autocracy for over a decade. With revelations since the 2003 conflict also casting doubt on President Bush's pre-war claims that Iraq held weapons of mass destruction and supported terrorism, it can be argued that the coercive denial strategy of 1990 had in fact been successful[342].

Taking a second more contemporary example which crosses the boundary between expeditionary war and COIN, the destruction of ISIS again illustrates the coercive denial strategy. Calling itself a caliphate, ISIS came to prominence in 2014 with its seizure of parts of Syria and Iraq. At its peak it ruled over 35,000 square miles and almost 8 million people[343].

[339] J. M. Broder and D. Jehl, "Iraqi Army: World's 5th Largest but Full of Vital Weaknesses", *Los Angeles Times*, 13 August 1990.
[340] J.W. Pardew, "The Iraqi Army's Defeat in Kuwait", *US Defence Technical Information Centre,* 17 (1991): 17.
[341] D. Byman, "After the Storm: Us Policy toward Iraq since 1991", *Political Science Quarterl,* 115, no. 4 (2001): 493.
[342] Bush's pre-war claims were most notably made in a radio address on 22 March 2003 when he famously stated that 'our mission is clear, to disarm Iraq of weapons of mass destruction, to end Saddam Hussein's support for terrorism, and to free the Iraqi people'. This statement was contradicted by the publication in 2005 of 'the Downing Street Memo' which confirmed that the US people had been misled.

G.W. Bush, "President's Radio Address: President Discusses the Beginning of Operational Iraqi Freedom", ed. The White House Archives (2003).

[343] For background on ISIS, see:

BBC, "The Rise and Fall of the Islamic State Group: The Long and Short Story", https://www.bbc.co.uk/news/world-middle-east-47210891.

H. Hassan, "The True Origins of Isis", *The Atlantic*2018.

In the battle that followed analysts agreed that the groups ideology could not be defeated. What was assessed as being vulnerable were the elements it required to run a state: a workforce, fiscal resources, and the ability to control and secure territory[344]. The loose global coalition which was formed to destroy these elements and achieve coercion through denial would include not only a US led group of states, but also Russia and an array of local forces from the Kurdish Peshmerga to the Syrian Army[345]. In delivery, the effect was decisive. Whilst, as predicted, ISIS was not necessarily destroyed and may re-emerge, the strategy of coercion through denial did succeed in the freeing of 8 million people previously under its control.

Given the contemporary relevance of this form of coercion, one must ask what military means are pivotal to its achievement. Whilst it cannot be denied that ground forces were essential to the above examples, the key capability for both the super and great power states involvement in these was air power.

Considering first the Gulf War in 1990, Coehn comments that the conflict represented the 'opening shot of a fundamental transformation in the nature of warfare'[346]. Referring to the effect of air power, this view was vividly illustrated by media images which graphically charted air power's employment in the opening days of the conflict as the Coalition's only offensive capability.

Replayed countless times on televisions throughout the world, tracer fire over Baghdad, the pinpoint accuracy of laser-guided bombs and the 'highway of death' where allied forces destroyed Iraqi ground troops all added to the picture[347]. Taken collectively, these horrific scenes showed not only the decisive nature of air power in coercion through denial but also, in US Secretary of Defense Richard Cheney's words, signalled a dramatic shift in what he labelled as the 'military-technological revolution in warfare'[348]. Beyond this, its use also dovetailed

[344] T.K. Kelly et al., *Knowing the Enemy* (Santa Monica: RAND, 2017), 2.

[345] For a summary of how ISIS was defeated, see:
R. Hall, "Isis Caliphate Defeated: How Did It Happen and Do They Still Pose a Threat?", *Independent*, 23 March 2019.

[346] Cohen, "Mystique of Us Air Power", 109.

[347] J.A. Winnefeld, P. Niblack, and D.J. Johnson, *A League of Airmen: Us Air Power in the Gulf War* (Santa Monica RAND, 1994).Int

[348] R. Cheney, interview by E.A. Cohen, 1994.

seamlessly into Byman et al's 'new norms' allowing the project objective to be achieved with limited casualties[349].

This argument for the dominance of air power in the approach of super and great states to coerce through denial is further supported by the conflict with ISIS. Commencing under Operation Inherent Resolve in August 2014 with the first US air strikes against ISIS targets, the loose coalition would by August 2017 have conducted over 24,500 air strikes. This consistent use of a single capability to project power and achieve deterrence through denial was unparalleled[350].

Including concerted air strikes against ISIS infrastructure and leadership, the strategy allowed these states to support local ground troops enabling them to overcome ISIS and do so in a manner that adhered to Bymans et al's 'new norms'[351]. Though, as commentators had predicted, this did not destroy the ISIS ideology, it did deny the ability to function as a viable 'state' and therefore further prove the pivotal utility of air power.

Reflecting on this discussion of coercion, it is evident that in achieving the project objective coercion through punishment is no longer relevant. Even though air power is ideally suited to it, it does not fit the 'new norms' of warfare and will therefore not be a factor that induces states to procure air power.

However, the concept of coercion through denial, and the role of air power within it, is an entirely different discussion. Ideally suited to the 'new norms', it allows states to project power without committing ground troops. Though admittedly reliant on local forces to deliver the necessary ground elements, it nonetheless presents an attractive option for Western states seeking to project without having to commit.

[349] Byman, Waxman, and Shapiro, "The Future of Us Coercive Airpower," 54.
[350] US, "Operation Inherent Resolve: Target Operations to Defeat Isis", ed. United States Department of Defence (2017).
[351] For a summary of the fighting against ISIS and the means it took to succeed (including the use of air power), see: D. Sagromoso, "Who 'Defeated' Isis? An Analysis of Us and Russian Contributions", *Russia Matters,* (2020).

Based on this, it is concluded that coercion will in this form remain central to super and great power strategies. Though such an effect can be achieved via other cost-imposing capabilities from the land, maritime and cyber domains, air power remains in the 21st century a pivotal capability able to deliver reliable, impactful coercion within an acceptable level of risk and cost to the state. Therefore, those states which seek a global role will continue to procure, and become reliant on, air power.

Promoting National Prosperity

Turning to the last objective and looking beyond the existential threats of protect and the hard power of project, states wishing to maintain a global role and status also routinely seek to promote. Defined by UK strategy as the intent to seize opportunities by working innovatively, the objectives core themes fall within the concepts of soft and, by association, smart power[352].

When translating this political aim into military means, the focus is multifaceted. In this, the military is recognised as a credible means to achieve persistent engagement with overseas partners. Demonstrating commitment to a global role, it can be argued that to contribute to stability within the international system, and foster mutual understanding via military engagement, it remains an important theme for all states[353]. This is because, as Nye suggests, it is logical to avoid the costs of conflict by co-opting rather than coercing[354].

Critics of soft power highlight that this is not the solution to all problems. Others go further suggesting that its advocates are naive to trust soft power because popularity is 'fundamentally ephemeral and should never guide foreign policy'[355]. However, whilst such criticisms are recognised, the reality is that states are increasingly employing soft and smart power to achieve political ends. Illustrated by examples including those discussed above such as Allied personnel

[352] UK, "National Security Strategy and Strategic Defence and Security Review: A Secure and Prosperous United Kingdom", 11.
[353] "Joint Doctrine Publication 0-30: Uk Air and Space Power, 2nd Ed", 15.
[354] Nye, "Public Diplomacy and Soft Power", 95.
[355] For further discussion on the criticisms of soft power, see:
Wilson, "Hard Power, Soft Power, Smart Power", 110.

developing post-war Japan and Germany, it is evident that the trend is well established[356].

Taken in the context of air power, which as discussed is encapsulated in Lowther's concept of 'air diplomacy', the strong argument for soft and smart powers utility continues[357]. Maximising air power's speed, reach and versatility, the logic follows that air power has a great deal to offer states who want to deliver soft power quickly and decisively. Eclipsing the abilities of land and maritime forces, it can be concluded that all super and great powers will continue to employ air power as a central aspect in their military's delivery of soft power. Though not as existential a discussion as the protect and project objectives, the drive to promote does add further weight to why states are likely to procure, and become reliant on, air power.

Limitations of the 'First Cause': Not an Absolute Requirement

The above discussion explored why states will procure and become reliant on air power. Achieving a 'golden thread' from the international system, through the nuances of power to its enablement of strategic objectives, a depth of argument was offered. However, it is recognised that there is no 'one size fits all' argument within the complexities of a realist-constructivist world. Therefore, to identify the boundaries of the 'first cause', this section will examine the limitations associated with states' reliance on air power.

To begin, it is acknowledged that despite its rise over the last century, the claim that air power can in isolation meet a state's requirement for military power is incorrect. A claim first made in the inter-war years by theorists including Douhet, it was contended that air power could through strategic bombing destroy an enemy's ability and will to fight[358]. Developed into the 21st century, some theorists continued the line of argument contending that modern precision increases the

[356] Keck, "The Hard Side of Soft Power".
[357] Lowther, "Air Diplomacy: Protecting American National Interests", 4.
[358] For Douhet's principal work, see:
Douhet, *The Command of the Air*.
For an in-depth discussion of Douhet's work, see:
Segrè, "Giulio Douhet: Strategist, Theorist, Prophet?".

ability of air forces to deliver a 'knockout blow'[359]. A position epitomised by Warden, he argued that any adversary can be understood as a series of concentric rings with on the outside military forces encasing the decreasing circles of population, infrastructure, processes and, at the centre, leadership. Employing this model, Warden concludes that modern precision air power allows a state to 'jump' the outer rings and directly strike an adversary's centres of gravity achieving strategic paralysis. At this point an adversary is prevented 'from repairing itself, protecting itself against future attacks, or making competent attacks against its opponent's systems' creating victory without the need to deploy land or naval forces[360].

Though Douhet and Warden enjoy mainstream recognition, others consider their arguments as 'the last word on air power extremism'[361]. Taking a more balanced view, Pape acknowledges that even with the precision of modern air power, the capability in isolation is unable to win conflicts[362]. When mapped across the above discussion of power, one observes that air power is one amongst many tools used in the military lever. The question to be addressed is therefore whether air power is essential to all states or if some have differing reliance's in maintaining their roles and assuring survival?

The first point to acknowledge in responding to this question is Pietrucha and Renken's assertion that 'air power may not win wars, but it sure doesn't lose them'[363]. Exploring this with reference to the US, they argue how in the 21st century the US departed from the successful post-Vietnam air power dependent template seen in the Former Yugoslavia to engage in unsuccessful ground-centric campaigns in Iraq and Afghanistan[364]. Despite the massive superpower

[359] R.S. Dudney, "Douhet", *Air Force Magazine*, April 2021.
[360] Warden, "Strategy and Airpower".
[361] Dudney, "Douhet".
[362] R. Pape, "The True Worth of Air Power", *Foreign Affairs,* 83, no. 2 (2004).
[363] M. Pietrucha and J. Renken, "Air Power May Not Win Wars, but It Sure Doesn't Lose Them", *War on the Rocks,* (2015).
[364] With reference to the importance of air power in the Former Yugoslavia, Tilford notes that in 'the wake of the 78-day NATO bombing campaign against Yugoslavia led by the United States, some air power enthusiasts trumpeted their success…[boasting] that this was the first-time air power and air power alone had defeated an enemy land army'.
E. Tilford, "Operation Allied Force and the Role of Air Power", *Parameters* Winter (2000).
For in depth analysis on why the Iraq and Afghanistan ground-centric campaigns were unsuccessful, see:
A.H. Cordesman, "America's Failed Strategy in the Middle East: Losing Iraq and the Gulf", *Center for Strategic and International Studies (CSIS),* (2020).
J.H. Lebovic, *Planning to Fail: The Us Wars in Vietnam, Iraq, and Afghanistan* (Oxford: Oxford University Press, 2019).

expenditure of both lives and finance spent in these latter conflicts, it is commonly agreed that the results were strategically questionable. Conversely, when the US returned to air power centric campaigns in Libya and Syria in support of local ground forces, strategic gains were achieved in short time scales[365].

Pietrucha and Renken's argument can be judged to indicate that if the US seeks to maintain its constructivist global superpower role it must focus resources 'away from the ground-centric, Army-heavy approaches that characterised Vietnam, Iraq, and Afghanistan' and toward the projection of air power[366]. A lesson replicable to great powers including the UK and France, it can be concluded that for states whose constructivist identity is tethered to projecting global power the loss or compromise of air power would put their role at risk.

For those states without global aspirations, this utility of air power is less relevant. Taking New Zealand as an example, this state holds a regionally focused foreign policy built on the four pillars of 'rules, architecture, relationships and diversification'[367]. Though in 2021 its national defence assessment recognised a need to shift these pillars from 'a predominantly reactive risk management-centred approach to one based on a more deliberate and proactive strategy', such a strategy remains regionally centric and reliant on the diplomatic and economic levers[368]. Therefore, in the case of New Zealand and similarly sized regional states without global aspirations, the loss or compromise of air power would not negatively impact its ability to maintain their national role[369].

Though this argument largely focuses on the expeditionary aspirations of global super and great powers, longer term conventional threats further prove the importance of air power. Challenging the Clausewitzian based premise that only land power can win wars, it is accepted that whilst air power cannot dominate,

[365] For discussions on the role of Western air power in Libya and Syria, see:
Mueller, *Precision and Purpose: Airpower in the Libyan Civil War* ; Sagromoso, "Who 'Defeated' Isis? An Analysis of Us and Russian Contributions"; Hall, "Isis Caliphate Defeated: How Did It Happen and Do They Still Pose a Threat?".

[366] Pietrucha and Renken, "Air Power May Not Win Wars, but It Sure Doesn't Lose Them".

[367] B. King, "Speech by New Zealand Secretary of Foreign Affairs and Trade", ed. New Zealand Government (2018).

[368] New Zealand, "Defence Assessment: A Rough Sea Can Still Be Navigated ", ed. Ministry of Defence (2021).

[369] For further discussion of New Zealand's regional role, see:
L. Pend, "New Zealand's Subtly Shifting Foreign Policy", *The Diplomat,* (2022).

taking and holding ground without air power is challenging[370]. Persisting in relevance, the use of air power in the 2003 invasion of Iraq to destroy all credible opposition illustrates this argument[371]. This is supported by lessons from the 2022 invasion of Ukraine in which Russia, lacking air superiority and largely limited to cruise and ballistic missiles, failed to achieve decisive strategic advantage[372].

These examples confirm that to both achieve conventional military effect and defend against aggression air power, and ideally air superiority, are essential. In mapping the relevancy of this statement, the importance is not limited to super and great powers such as the US, UK and France who may wish to protect power. Rather, in the wake of Russia's invasion of Ukraine and the PRC's expansionist tendencies many states have increasingly recognised the need for air power. Proven by significant investment, examples include Germany and Finland who, facing a resurgent existential threat, have reversed previous orders for ageing F-18 aircraft in preference for the advanced F-35[373]. Mirrored in the Asia-Pacific by Japan's purchase of the F-35 and Taiwan's modernisation of its F-16 fleet, the reinforcement of air power as a pivotal capability by a predominance of states is evident[374].

Conversely, not all states have either the role which would require power projection into conventional conflicts, nor an existential threat. Ireland, for example, maintains a small Air Corp charged with contributing 'to the security of the State by providing for the Military Air Defence of its airspace'[375]. With no

[370] For an analysis of Clausewitzian inspired thinking on land power and its necessity in gaining, sustaining, and exploiting control over land, resources, and people, see:
K.P. Adgie, "Applying Clausewitz to 21st Century Landpower Theory", (US Army War College 2010).

[371] For the value of air power in the 2003 Iraq conflict, see:
Ullman, "War in Iraq: Shock and Awe Revisited".

[372] For analysis of the Russian strategic limitation in its 2022 invasion of Ukraine and the importance of air power, see:
J. Bronk, N. Reynolds, and J. Watling, "The Russian Air War and Ukrainian Requirements for Air Defence", (RUSI, 2022).

[373] For discussion and analysis of the German and Finnish procurement of the F-35, see:
V. Machi, "State Department Approves $8.4 Billion F-35 Sale to Germany", *Defense News*, 22 July 2022.
E. Lehto and M. Stone, "Finland Orders 64 Lockheed F-35 Fighter Jets for $9.4 Bln", *Reuters* 10 December 2021.
V. Machi, "How the F-35 Swept Europe, and the Competition It Could Soon Face", *Defense News* 4 September 2022.

[374] For comment on the Japanese purchase of the F-35, see:
Defense Security and Cooperation Agency, "Japan - F-35 Joint Strike Fighter Aircraft ", (2020).
K. Osborn, "Japan Launches F-35b from Destroyer - to Neutralize China's Fleet of J-20 & J-31 Fighter Jets", *Warrior Maven* 29 July 2022.
For the expansion of Taiwanese air power, see:
Staff Writer, "Taiwan Gives up on F-35, Turns to F-16v Option", *The National Interest,* (2018).

[375] Ireland, "Air Corps", ed. Irish Defence Forces (2023).

indication that the threats it faces will become existential, and the UK already providing air policing in Irish airspace, the loss or compromise of Irish air power would have minimal impact on its role or survival[376].

Reflecting on the examples of New Zealand and Ireland, it is evident that any blanket application of this 'first cause' in which states procure and become reliant on air power is incorrect. With all states unique, and the realist-constructivist world complex, some states without global aspirations or existential threats will not become reliant on their own national air power. However, where global influence remains entwined with a state's role or a credible existential threat exists, the 'first cause' manifests and states will procure and become reliant on air power to assure their role and, in extremis, survival. Therefore, the 'first cause' has been shown to not be absolute but, where it applies, remains a relevant element of air power's cyber risk.

Conclusion

This Chapter introduced, explored, and justified the proposed 'first cause' of air power's cyber risk: states' procurement of, and reliance on, air power. Beginning with an exploration of the contemporary international system, core IR assumptions on states' primacy and the rising influence of non-state actors were discussed. Though concluding that even in a 'post-Westphalian' reality states retain primacy, it was accepted that in its exploration of air power the thesis should not be blinkered and ensure that non-state influences are, where relevant, examined.

Next considering the concepts of power and influence, it will be acknowledged these as forming the core of not just this thesis, but all discussions of IR. In recognition, it was asserted that in the context of states any examination of these concepts must focus on one specific question: 'power over whom, and with respect to what?'[377].

[376] G. Allison, "Do British Fighter Jets 'Protect' Irish Airspace?", *UK Defence Journal* (2022).
[377] Jablonsky, "National Power", 34.

Cautioning against the contested nature of this long running discussion on power, it was subsequently accepted that attempts to secure 'a single, consistent, coherent 'Theory of Power'' were impossible[378]. In response, Hart's argument was identified as instructive. Acknowledging the limitations, Hart was shown as not seeking a single definition but a measure of the indicators of power by dividing them into whether states seek control over resources, actors or events and outcomes[379]. Adopting this it was concluded that power in isolation has no value, but it is a state's motivation and subsequent ability to harness power through influence that is pertinent.

Building on this understanding, the motivation of states to harness power and create influence was explored in the context of the realist-constructivist framework. Illustrating why both the individual elements of realism and constructivism have relevance, it was concluded that by combining their 'interlocking pieces' the thesis would solve the larger IR puzzle[380].

With this foundational framework in place, it was next considered how, with specific reference to air power, states harness power to achieve influence. Led by Nye's 'stick', 'carrot' and 'attractions' analogy, the issues were addressed by introducing the instruments of power[381]. With the diplomatic and economic instruments initially considered, the military instrument was identified as offering states the most pivotal effect. Pairing this down to its hard, soft, and smart components, the role and importance of air power to the achievement of each was explored.

In the first, hard power was identified as forming the natural focus of the military instrument. Employed to coercive effect through the threat or use of force, the utility of all military capabilities was noted before identifying that for over a century air power has been the most impactful. Proving the predictions of early air power

[378] Dahl, "The Concept of Power", 202.
[379] Hart, "Three Approaches to the Measurement of Power in International Relations".
[380] Lebow, "Constructive Realism", 346.
[381] Nye, "Public Diplomacy and Soft Power", 94.

theorists, and evidenced by numerous modern conflicts, it was concluded that air power delivers a unique ability to achieve strategic intent. Given this, the discussion asserted that in their quest to hold hard power capabilities, states will be driven to procure, and become reliant on, air power.

Though important, it was further acknowledged that while 'hard power may offer a solution to one problem, it may undermine attempts to solve others'[382]. Given this, states' pursuit of soft power through the military instrument was discussed. Identifying it as the art of 'getting others to want the outcomes that you want' through co-option rather than coercion, soft power was acknowledged as an important activity for all states[383]. Recognising in this that both land and maritime forces have utility, it was concluded through a discussion of Lowther's concept of 'air diplomacy' that air power offers the unique advantages of speed, reach and versatility[384]. By virtue of these qualities, air power was, through soft power, again identified as a capability that states are likely to become reliant on.

Turning next to discuss smart power, a term defined as the capacity to combine hard and soft power in a mutually reinforcing manner[385], the Chapter noted the importance the military instrument plays. Reflecting on the centrality of air power to hard and soft power, it was concluded that this utility naturally extends to smart power.

Having confirmed the role of air power in states' harnessing of power, the Chapter next sought to underline the capabilities' vital importance to modern states. Providing a final piece to the 'puzzle' of the 'first cause' of air power's cyber risk, the discussion examined how the motivation for power and influence has translated into a pivotal role for air power. Framing the discussion by outlining the fundamentals of military strategy and how this is expressed through strategic objectives, the use of three key themes to structure the discussion was identified: protection of sovereignty, projection of global power and promotion of prosperity.

[382] UK, "Joint Defence Doctrine 0-01 Uk Defence Doctrine", 3.
[383] Nye, "Public Diplomacy and Soft Power", 95.
[384] Lowther, "Air Diplomacy: Protecting American National Interests", 4.
[385] Wilson, "Hard Power, Soft Power, Smart Power", 115.

Reflecting on these three aspects in combination, it was ultimately argued that in the realist-constructivist sense states must effectively harness power and achieve actionable influence over resources, actors or outcomes and events to survive and thrive. Though this can be achieved across all the instruments of power, it was shown how the military instrument is, and will always be, decisive in a world influenced by realist motivations. With air power shown to hold a decisive role within this instrument, an overarching theme was confirmed: to survive and thrive states must procure, and will become reliant on, air power.

Despite the strength of the collective argument, it was finally acknowledged that as this ‘first cause’ is not absolute it cannot be used as a blanket rule for all states. Exploring examples, it illustrated how the cause was not applicable to smaller states with no intent toward global power projection or not facing an existential threat. However, for others whose role is entwined with global relevancy or those who face an existential threat, the argument that they will procure and become reliant on air power remains relevant.

Establishing the validity of this proposed ‘first cause’ of air power’s cyber risk, the discussion has shown the capabilities’ unique centrality in assuring relevant state’s role, status, and survival. However, what was not achieved was a justification of why, amongst all the dangers that exist in the modern world, cyber represents the most likely means through which an adversary could reduce the strategic viability of air power. To address this, the thesis will, in the following chapters, explore the proposed second and third causes of air power’s cyber risk: cyber vulnerabilities of, and threats to, air power.

Chapter 5: The 'Second Cause' - Digitally Exploitable, Air Power's Cyber Vulnerabilities

Introduction

The previous Chapter showed air power to be a keystone capability within the realist-constructivist explained drive for states to survive and thrive. What has not been explored is the increasing degree to which air power is reliant on digital technologies and, by association, is vulnerable to digital exploitation by hostile actors. Forming the foundation of the proposed second cause of air power's cyber risk, cyber vulnerabilities, it is these concepts that this Chapter will explore. Specifically, how significant are air power's digital vulnerabilities and, if exploited, could they cause its loss as a strategically viable capability?

Introducing this discussion, the concept of cyber vulnerabilities will initially be explored. In this, it will be identified as a continuation of the modern trend to link digitisation with a specific concept using cyber as a prefix. Having explored differing interpretations of this nomenclature it will be concluded that any consideration of cyber vulnerabilities must include not only the core elements of software and hardware, but also human-machine interaction and the cognitive space in which people interact.

Reinforcing the 'Layers of Cyberspace' model as a facilitator to exploring this holistic view, the people, information, and real layers will in turn be explored[386]. Employing relevant examples to articulate the potential impact that cyber vulnerabilities have within each, the topic's inclusion in the wider discussion of cyber risk will be justified. Specifically, it will be shown how at each layer cyber vulnerabilities provide the digital avenues through which air power can be targeted.

Finally, having reviewed the discussion, the Chapter will conclude by acknowledging that whilst cyber vulnerabilities are concerning, any standalone

[386] UK, "Cyber Primer", 5.

discussion of them is incomplete. To fully understand the risk posed to air power and provide an answer to whether this thesis' predictions have value, a further discussion on cyber threats is required. This is because, even if cyber vulnerabilities are creating digital avenues to disrupt air power, none are of concern without the existence of hostile actors with the capability and intent to exploit them.

Understanding and Modelling Cyber Vulnerabilities

To understand cyber vulnerabilities, it is first necessary to examine the concepts that underpin the term. With technology actively shaping our lives, one might assume that we already have this understanding[387]. However, in a similar vein to misconceptions on the wider terminology of cyber, cyber vulnerabilities are themselves not always fully understood.

In beginning this examination, it is noteworthy that mirroring the wider topic the term cyber vulnerabilities is an evolution of the modern practice of using cyber as a prefix to denote digital technologies. Based on this modern lexicon, it is logical that exploitable weaknesses in digital technologies are referred to as cyber vulnerabilities. Though intuitive, the term alone does not provide an understanding of the concept. Rather, as with wider discussions of cyber in which much terminology is yet to be definitively understood, what is meant by cyber vulnerabilities is itself not universally agreed[388].

To address this one must first consider what is meant by vulnerabilities. At its broadest level, the International Standards Organisation (ISO) defines vulnerabilities as 'intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence'[389]. Refined in a digital context, the US National Institute for Science and Technology (NIST) defines a

[387] Discussing the impact of technology on our daily lives, Birdle comments that it is no longer 'merely augmenting our lives…[but] shaping and directing them'.

Bridle, "Rise of the Machines: Has Technology Evolved Beyond Our Control?".

[388] Futter delivers an informative discussion on how the meaning, scope and nature of the term cyber and its associated terminologies are yet to be decided.

Futter, "Cyber Semantics: Why We Should Retire the Latest Buzzword in Security Studies", 216.

[389] ISO, "Iso Guide 73: 2009 – Risk Management (Vocabulary) ", (2009).

vulnerability as being 'a flaw or weakness in systems' security procedures, design, implementation, or internal controls that could be exercised and result in a security breach or a violation'[390]. Though both use impenetrable language, they share a basic premise: a vulnerability is a weakness which if exploited by a hostile actor may cause loss or damage. The importance of understanding vulnerabilities is therefore clear. Specifically, an organisation may have assets of value, and a hostile actor may have the intent and capability to target them, but if vulnerabilities cannot be exploited an attack will fail.

The role of those protecting digital systems should therefore be equally simple: identify and remove all vulnerabilities. However, as the UK's National Cyber Security Centre (NCSC) comments, 'this can be easier said than done'[391]. To remove all digital vulnerabilities, one must isolate a system from the outside world, remove physical connections and place it in a faraday cage[392]. Though effective, such actions also remove operational utility[393].

As abolishing vulnerabilities is not practicable, defenders must identify and manage them. To achieve this security professionals employ information security standards as a guide to identifying exploitable vulnerabilities[394]. Though these standards routinely direct the use of generic tools such as document reviews[395]

[390] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems: Recommendation of the National Institute of Standards and Technology ", in *Special Publication 800-30* (National Institute of Standards and Technology 2002), 2.

[391] UK, "The Fundamentals of Risk ", (. National Cyber Security Centre, 2019).

[392] A faraday cage is 'an enclosure made of conductive materials which is capable of blocking external electric fields'. In simple terms, a digital system placed inside a faraday cage cannot be accessed remotely or interfered with by anything outside that environment. This allows the removal of system vulnerabilities.

Techopedia, "Faraday Cage", (2019).

[393] Examples of where systems and networks are maintained in closed environments include test beds used for software development which 'test and evaluate prototypes…[and] de-risk projects'. Because such environments mirror the real-world but in an enclosed and controlled manner (much like a laboratory), no onward network connections are required. Alongside other peripheral examples such as standalone intelligence networks were the ingress and egress of information is tightly controlled, there are limited examples of where a network or system can be entirely disconnected from the outside world whilst concurrently retaining operational value.

K. F. Joiner et al., "Four Testing Types Core to Informed Ict Governance for Cyber-Resilient Systems", *International Journal of Advances in Security,* 11, no. 3 (2018): 314.

[394] For an overview of the procedures which can be used to identify vulnerabilities in information systems, see:

Stoneburner, Goguen, and Feringa, "Risk Management Guide for Information Technology Systems: Recommendation of the National Institute of Standards and Technology ".

[395] Johnson notes that security documentation reviews 'determine if the technical aspects of policies and procedures are current and comprehensive. These documents provide the foundation for an organisation's security posture but are often overlooked during technical assessments'.

L. Johnson, *Security Controls Evaluation, Testing and Assessment Handbook* (Amsterdam: Elsevier), 7.

and penetration testing[396], approaches vary depending on the system[397]. Whilst this may suggest a breadth of thinking, the reality is that virtually all frameworks are blinkered by their technical nature. The result is a tendency for narrow examinations to allow broader vulnerabilities to go unnoticed.

To address this issue, and judge how widely cyber vulnerabilities should be considered, we must examine how both cyber and therefore its vulnerabilities have been defined. With dozens of subjective alternatives already offered[398], it is necessary for brevity to divide the definitional groups into two broad camps: system and network centric definitions and holistic definitions.

Endorsing the first, Nye states that cyber should be considered 'a prefix standing for electronic and computer related activities'[399]. Supported by Kuehl who defines cyber as being framed as the use of electronics[400], these academic approaches are representative of most governmental thinking[401]. Given this, one might assume that there is broad agreement that any consideration of cyber and its vulnerabilities should be limited to the hardware and software that constitutes systems and networks.

[396] Penetration testing is defined by the NCSC as 'a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might'. As noted by McDermott, penetration testing is now considered 'a fundamental aspect of information system security'. For quotes and depth, see:

UK, "Penetration Testing ", (National Cyber Security Centre, 2019).

R.R. Linde, "Operating System Penetration", in *National Computer Conference and Exposition* (1975).

J.P. McDermott, "Attack Net Penetration Testing", in *Proceedings of the Workshop on New Security Paradigms* (2001), 1.

D. Khan, *The Most in-Depth Hackers Guide: Hack Like a Pro!* (North Carolina: Lulu.com, 2015), 18.

[397] Stoneburner, Goguen, and Feringa, "Risk Management Guide for Information Technology Systems: Recommendation of the National Institute of Standards and Technology ", 15.

[398] Discussing the definitions of cyber, Nye comments that any definitive understanding is made challenging by the fact that there are literally dozens of versions to choose from. This is underlined by Futter who comments that because debates in this area remain 'in the eye of the beholder' the identification of a single definition all can agree on is virtually impossible.

Nye, *Cyber Power*, 3.

Futter, "Hacking the Bomb: Nuclear Weapons in the Cyber Age", 4.

[399] Nye, *Cyber Power*, 3.

[400] Kuehl's full definition of cyber is as the 'use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies'.

Kuehl, "From Cyberspace to Cyber Power: Defining the Problem," 4.

[401] For example, the US *National Security Strategy to Secure Cyberspace* defines cyber as an environment 'comprising hundreds of thousands of interconnected computers, servers, routers, switches, and fibre optic cables'. This definition has guided much other US official thinking on the topic including the US military definition of cyber as being 'characterised by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems'. Collectively, these approaches are representative of most governmental interpretations of cyber both in the US and elsewhere.

US, "The National Strategy to Secure Cyberspace", 1.

"National Military Strategy for Cyberspace Operations".

This interpretation has however been disputed by the holistic definitions. Futter, for example, suggests that the 'cyber challenge' should be thought of as not just comprising software and hardware but also the people who engage with them[402]. This assertion is given depth by Singer and Friedman who acknowledge that whilst cyber is a digital environment, it is not purely virtual. Rather, as it is man-made, and society has been fundamentally altered by interaction with it, cyber must be defined as much 'by the cognitive realm as [it is] by the physical or digital'[403].

Reflecting on these arguments it is acknowledged that any analysis of air power's cyber vulnerabilities must include the core elements of software and hardware in both their digital and physical manifestations. However, to be comprehensive discussions must go further and consider both human-machine interaction and the cognitive space in which people interact with, and exist in, the digital world. Though adoption of this may define the scope to which we should consider cyber vulnerabilities, it fails to provide a framework through which research can examine the topic. To achieve this, a cohesive model is required.

In searching for this, a variety of options can be considered. One example is the creation of a cyber topography to map cyber vulnerabilities. Meaning, in its original sense, the study of the Earth's surface[404], the co-option of topography into cyber has seen it used to correlate virtual locations with actual experiences[405]. Despite contextualising the cognitive elements of cyber, Nunes suggests that because the approach is 'virtual' it fails to chart the 'real'[406]. As cyber cannot be divorced from its physical manifestations, the approach is too limited to be of value.

A second more technical option is the Open Systems Interconnection (OSI) model. A conceptual description of systems, it partitions technologies into seven

[402] Futter, "Hacking the Bomb: Nuclear Weapons in the Cyber Age", 4.
[403] Singer and Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* 14.
[404] Mapscapping.com, "What Is Topography? ", https://mapscaping.com/blogs/news/what-is-topography.
[405] For a discussion of how the concept of topology has been applied to cyber, see:
M. Nunes, "Virtual Topographies: Smooth and Striated Cyberspace," in *Cyberspace Textuality: Computer Technology and Literary Theory* ed. M. Ryan (Indiana: Bloomington, 1999).
[406] Ibid., 429.

interconnecting layers which provide a path for information to traverse networks[407]. Though inclusive, Bauer and Patrick comment that the model is incomplete[408]. Technology centric, its focus on data makes it 'invisible to users' and therefore ineffectual for the purposes of this research[409].

Moving next to academic approaches, a promising option is that of cyber littorals. Adopting an oceanographic term, the littoral commonly describes the area of water near the shore and the area of shore near the water[410]. Applied to cyber by Withers, its meaning is adapted to describe the point at which 'the hardware and software of cyberspace come into contact with the physical and cognitive world'[411]. Though explaining the edges of cyber, and therefore where cyber vulnerabilities are found, Withers acknowledges that if all elements were included in the 'cyber littoral zone' the grouping would become so large that the model would no longer have value[412].

A solution to cyber's unwieldy size is offered by Futter who categorises cyber activities into three areas: physical, logical, and human[413]. Whilst elegant, a more comprehensive model following similar logic is provided by UK military doctrine. Specifically, the *Cyber Primer's* 'Layers of Cyberspace' model describes cyberspace as a complex, dynamic and 'all-encompassing operating environment'[414]. Further examining the environment, the model provides the context necessary for this research by subdividing cyber into three layers: people, information, and real[415].

With the resultant framework outlining clear sub-divisions which reflect this thesis' definitional perspective, it provides a cohesive model through which to explore

[407] G. Bora et al., "Osi Reference Model: An Overview", *International Journal of Computer Trends and Technology (IJCTT),* 7, no. 4 (2014): 214.

[408] B. Bauer and A.S. Patrick, "A Human Factors Extension to the Seven Layer Osi Reference Model", *Nortel Networks Research*: 1.

[409] Ibid.

[410] Peters and Lodge, "Littoral Zone."

[411] Withers, "What Is the Utility of the Fifth Domain?", 133.

[412] Withers includes the following elements as being among those which should be considered to be in the cyber littoral zone: 'physical infrastructure, cabling and electrical power; the electromagnetic spectrum that data traverses; electro-mechanical processes under computer control; and the senses and cognition of computer users'.
Ibid.

[413] Futter, "Hacking the Bomb: Nuclear Weapons in the Cyber Age", 4.

[414] UK, "Cyber Primer", 5.

[415] Ibid.

cyber vulnerabilities. That said, it is also recognised that the adoption of models proffered by military doctrine for academic analysis can be problematic. Notably, such a decision may lead to accusations of the research being artificially narrowed because of the models being developed with pre-determined motivations. However, when considered against the background of academic discussion on cyber vulnerabilities explored above, it is asserted that the 'Layers of Cyberspace' model offers the most cohesive and in-depth characterisation of the question posed by this Chapter: what is the full remit of cyber vulnerabilities which contemporary air power is exposed to, and how concerned should states be about them?

Based on this, the following sections will explore each of the 'layers' offered by the model with a view to addressing the question posed. By doing so the thesis will continue to build an in-depth assessment of air power's cyber risk.

The People Layer

The Importance of People

With technology ingrained in the delivery of air power, and digital information cited as 'the lifeblood of Defence', people may not appear to be an intuitive starting point for a discussion of cyber vulnerabilities[416]. However, even though advances in technology continue to be driven by Moore's Law, a prediction that digital processing power will on average double every two years, conceptions of true digital autonomy remain the purview of futurology[417].

In the context of Defence, commentators argue that increasing automation and the introduction of Artificial Intelligence (AI) will in time reduce or even replace the role played by people. For air power, as Chaturvedi et al highlight, a notable area for such developments are UAVs that are increasingly replacing manned aircraft.

[416] UK, "Joint Service Publication (Jsp) 441 – Managing Information in Defence – Part 1: Directive", 1.

[417] For Moore's Law, see:

Moore, "Cramming More Components onto Integrated Circuits".

Futurology provides perceived and envisioned future realities. For depth, see:

P. Malaska, "Knowledge and Information in Futurology", *Foresight: The Journal of Future Studies,* 2, no. 2 (2000): 239.

Notwithstanding their growing use, contemporary UAVs are not controlled by AI or autonomous in the true sense. Rather, with people remaining pivotal at every step of air power from development through to operation, whether manned or unmanned, Dear concludes that true autonomy in aviation remains confined to the future[418].

Reflecting realities of this, people continue to be recognised by both academia and operators as intrinsic to air power. Taking the senior leadership of the RAF as an example, Air Chief Marshall Sir Stephen Hillier, Chief of the Air Staff from 2016 to 2019, built his 2017 strategy on the importance of people. Setting this out in his first line, Hillier asserted that 'people are at the heart of everything we do'[419]. Echoed in other organisations, the US Air Force (USAF) Chief of Staff for Personnel commented in 2010 that his organisation readily recognised people 'as its greatest asset'[420].

With the value of people to air power readily accepted, it is therefore of no surprise that the human relationship with technology is also reflected in the 'Layers of Cyberspace' model[421]. Identifying people as entwined with technology through the details that connect us to cyberspace and our interactions with networks, strong parallels can be found in Singer and Friedman's holistic definition of cyber that was discussed above[422].

Based on these arguments we can collectively conclude that this human element of air power reinforces the assertion that the digital world is not only made by people, but is driven by people. To explore what this means for air power's cyber risk, this section must first understand the people who create, operate, and interact with the digital environment. Once achieved, the Chapter can finally seek to understand the cyber vulnerabilities that are intrinsic to these interactions.

[418] Dear, "Artificial Intelligence and Decision-Making", 18.
[419] S. Hillier, interview by Royal Air Force, 2017.
[420] R.Y. Newton, interview by C. N. McLuney, 17 September 2010.
[421] UK, "Cyber Primer", 5.
[422] Ibid.

Outsiders

In addressing the issue of how people interact with the digital environment, the opening question revolves around the sheer scale of mankind's contemporary interaction with technology. Making it untenable for this discussion to consider a simple category of 'people', one must narrow the scope. This is most pragmatically achieved by distinguishing between 'outsiders' and 'insiders'.

Considering the first group, outsiders, the category is intuitively understood as anyone external to an organisation. In the context of technology, outsiders are more prescriptively defined as those with hostile intent who seek protected information from target organisations[423]. In adopting this interpretation, one confirms that outsiders are not a vulnerability but a threat. Therefore, though important to this research, the category is more appropriately encased in the following discussion of cyber threats.

Insiders

Having limited the scope of this discussion to insiders, we are presented with a group defined as those with legitimate access to an organisation's sensitive material[424]. With such individuals presenting a vulnerability for thousands of years, it is unsurprising that their impact has been actively discussed since the earliest digital technologies[425]. For example, in the 1960s the vanguard of digital technologies were resource sharing networks such as the US military ARPANET. Growing to nearly 60 nodes at geographically dispersed sites by the mid-1970s, ARPANET delivered significant connectivity and previously unparalleled utility. However, in equal measure, those responsible for such systems also recognised that they were allowing insiders an increasing amount of access to the data of

[423] This interpretation of an outsider in the context of cyber risk is taken from several industry and academic discussions. Of note, see:

A. Ja, "Insider Vs. Outsider Threats", *Infosec,* (2015).

Z. Hamin, "Insider Cyber-Threats: Problems and Perspectives", *International Review of Law, Computers and Technology,* 14, no. 1 (2000): 109.

[424] Homoliak et al., "Insight into Insiders and It: A Survey of Insider Threat Taxonomies, Analysis, Modelling and Countermeasures", 3.

[425] Crowdy articulates this assertion that people have posed a threat for thousands of years by commenting that the earliest surviving record of an insider can be traced to c.1274 BC.

Crowdy, *The Enemy Within* 19.

numerous sites and organisations. Shifting from one person having access to a single filing cabinet full of papers, a user at one terminal could access digital information from across all the connected organisations. The potential impact of a single breach therefore rose immeasurably[426].

Notwithstanding this early recognition, it was not until the 1990s that the digitally enabled insider vulnerability came to the fore. This change is most clearly epitomised by a transition from the operation of closed networks to the use of the internet as a bearer for digital links between networks[427]. Though globally impactful, the enormity of this change and its marked impact on the military has been characterised as ranging from a RMA[428] to a less seismic but still important shift in operational advantage[429]. Whichever phraseology is used, and without delving into the nuances of such definitional debates, it remains possible to conclude that the associated transition from platform to network-centric warfare had a notable impact on not only military capabilities, but also the insider vulnerability[430].

In the context of air power, this impact is most acutely evidenced by the 1991 First Gulf War. Facilitated by new networked ground and air systems, these technological shifts have been characterised as a seminal point in the development of the capability. Explored by Renner and developed by Olsen, both argue that in transforming air power's ability to provide and act on timely and accurate information, the US led Coalition was able to achieve air superiority and incapacitate Iraq's senior leadership in a single night[431]. Arguably unheard of in the history of armed conflict, this decisive ability to deliver 'deadly violence with

[426] Tarnoff, "How the Internet Was Invented".
[427] B.M. Leiner et al., "A Brief History of the Internet", in *ACM SIGCOMM Computer Communication Review* (2009), 23.
[428] Cebrowski and Garstka, "Network-Centric Warfare: Its Origin and Future", 29.
[429] For example, Libicki suggests; 'to argue that cyber warfare can have a revolutionary effect on the battlefield requires establishing that digital networking is itself revolutionary…[but] this is a step that many proponents of cyber…neglect to take'.
Libicki, "Why Cyber War Will Not and Should Not Have It Grand Strategist", 24.
[430] Steinnon's discussion of changes in technology in the 1990s highlight the shift from military organisations using technology to enhance the capabilities of a single platform to allowing connectivity across multiple platforms. This is characterised as a shift from platform-centric to network-centric warfare.
R. Steinnon, "Cyber Pearl Harbour Versus the Real Pearl Harbor", *Forbes* 7 December 2017.
[431] R.A. Renner, "America's Asymmetric Advantage: The Utility of Airpower in the New Strategic Environment", *Defence Studies,* 4, no. 1 (2004): 96.
J.A. Olsen, *Strategic Air Power in Desert Storm* (London: Routledge, 2003), 233.

greater speed, range and precision' than ever before has been characterised by Grey and Sloan as the 'coming of age' of military aviation[432].

Though historically significant, these developments were also notably accompanied by a necessary evolution in working practices. Resulting in most personnel gaining routine access to military digital systems, changes enhanced efficiency but concurrently increased the potential for insiders to cause harm. By the early 1990s this led to insiders being recognised as not only the principal vulnerability to networks but, due to the increased reliance on these networks, a significant vulnerability to operations[433]. Exploring this in depth, Hochberg et al conclude that when aligned to the system-specific knowledge of a skilled and trusted employee, the insider had from the early 1990s become the most concerning of all cyber vulnerabilities[434].

Three decades later this assessment remains central to contemporary discussions of cyber vulnerabilities. For example, writing in January 2020 Bunker commented that in the preceding 12 months internal errors caused by people were the root cause of half of the cyber breaches reported by US companies[435]. An assertion supported by Fielding, the insider problem remains, he assessed, 'the largest unresolved issue in cyber security'[436]. When underpinned by original research on the topic conducted by respected cyber security companies including Securonix and Splunk, the concern for all industries including defence is stark[437]. Specifically, as Moschovitis articulates, no matter how advanced technology becomes, insiders will remain the single most prevalent point of failure. This assertion is labelled by Moschovitis as the 'people singularity'[438].

[432] The quote on the 'deadly violence' of air power is from:
J.S. Nye and W.A. Owens, "America's Information Edge", *Foreign Affairs,* 75, no. 2 (1996): 23.
For depth, see:
C. S. Grey and G. Sloan, *Geopolitics, Geography and Strategy* (London: Routledge, 2013), 63.

[433] L.E. Bassham and T.W. Polk, "Threat Assessment of Malicious Code and External Attacks", (National Institute of Science and Technology (NIST), 1992), 11.

[434] Hochberg et al., "Addressing the Insider Threat", 4.

[435] G. Bunker, "Targeting Cyber Attacks: How to Mitigate the Increasing Risk'", *Network Security*, no. 1 (2020): 17.

[436] J. Fielding, "The People Problem: How Cyber Security's Weakest Link Can Become a Formidable Asset", *Computer Fraud and Security,* 6 (2020).

[437] Seuronix, "Insider Threats: Why It Continues to Matter Today", (2020), 1.
Splunk, "It Security Predictions 2020", (2020), 1.

[438] Moschovitis, "Why So Cyber Security Programmes Fail?", 308.

Recognising that this insider discussion is broad in nature, its application to air power is as relevant as it is to all industries. With, as explored above, air power continuing to rely on people to deliver even the most autonomous of UAVs, the ability of those within the organisation to cause harm to operational delivery is significant. Enhanced immeasurably by the previous discussion on the RMA of the 1990s, air forces are now at a position where such insider actions could not just damage but cease operations in the most extreme of circumstances. However, even when air power's vulnerability to the 'people singularity' is recognised, insufficient granularity is achieved to fully understand, measure, or manage the issue. To achieve this, a further sub-division between non-malicious and malicious insiders is required.

Non-Malicious Insiders

Considering the first, non-malicious insiders can be defined as those without hostile intent who through action or inaction cause harm[439]. With manifestations ranging from the mistaken publication of sensitive information to the accidental loss of devices, it presents a frustrating reality for organisations who must through necessity consider their people to be a risk rather than a resource[440].

This issue is no less real for air power. Reliant on the exploitation of digital information to deliver operations, air forces must trust their people with authorised access both in secure environments and, increasingly, outside the workplace through the use of military issued portable devices[441]. Compounded by the ability of personal smart devices to digitally capture sensitive information via voice, images or data, opportunities for the non-malicious vulnerability to manifest are extensive.

[439] Nurse et al., "Understanding Insider Threat: A Framework for Characterising Attacks", 214.

[440] A. Adams and M.A Sasse, "Users Are Not the Enemy", *Communications of the ACM,* 42, no. 12 (2010): 40.

[441] The USAF Office of Special Investigation (OSI) for example acknowledges the increased use of portable devices by their personnel though increased education campaigns on how to manage associated vulnerabilities. These vulnerabilities, the OSI highlights, range from criminal theft to the targeting of personnel by FIS.
US, "Office of Special Investigations Guidance - Travelling with Laptops and Mobile Devices", ed. US Air Force (2017).

To explore the relevance of this to air power, it is necessary to consider how this vulnerability might be realised and the consequences that may follow. Beginning with the most direct, media reports confirm the routine loss of military devices. For example, the UK Government confirmed that its MOD had in financial year 2017 to 2018 lost, through negligence, 30 desktop computers, 81 laptops and one tablet[442].

Though the consequences of such losses are seldom reported, examples in the public domain highlight the issue's importance. For example, in 1990 a UK military laptop containing operational plans, including air operations to support the intended removal of Iraqi forces from Kuwait, was negligently left in a car and subsequently stolen on the eve of the first Gulf War. Whilst sensitive information is not believed to have been compromised on this occasion, the potential impact of such a breach is deeply concerning for those seeking to secure the operational viability of air power. When reinforced by other known non-malicious insider breaches including the theft of a laptop in 2000 from the home of UK Armed Forces Minister John Spellar, the potential depth of the issue becomes clear. Specifically, there is no doubt that a non-malicious insider vulnerability could in the right combination of circumstances lead to a breach of sensitive information that directly damages air operations[443].

Losses do not however need to contain operational information to adversely impact air power. For example, the UK Security Services (MI5) comment that personal information can, if accessed by a hostile Foreign Intelligence Service (FIS), be used to identify and recruit individuals. These recruits, MI5 notes, may for personal or ideological reasons act as agents and secretly pass on information[444].

[442] T. Ellwood, "Ministry of Defence Computers: Written Question - 141014", in *Written Questions and Answers*, ed. UK Parliament (2018).
[443] For depth on the non-malicious insider breaches noted, see:
A. Bloxham, "History of Recent Data Blunders by Government", *The Telegraph*, 14 October 2011.
M Taylor, "Lost Laptops, Disks and Dossiers", *Independent*, 15 June 2008.
[444] UK, "How Spies Operate ", (Security Service (MI5), 2020).

Despite public discussions in this area being limited, it is known that both the UK and US militaries have lost large amounts of personal data[445]. If such information were accessed by a hostile FIS, it is possible that the detail could be used to recruit agents who might cause long-term damage to a state's air power. This scenario is shown to be viable through the example of USAF airwoman Monica Witt who was recruited and subsequently passed sensitive information to Iran. Based on this, it can be concluded that losses which facilitate the recruitment of agents, but not direct harm, can have just as significant an impact on the viability of air operations[446].

Concerning in themselves, these are not the only manifestations of the non-malicious insider vulnerabilities in air power. In a further example, the vulnerability is not realised through error but because of outsiders targeting insiders. This process known as social engineering is defined by Ghafir as the 'ultimate psychological manipulation technique used by attackers to generate responses from unwilling targets'[447]. When employed successfully, the consequences of social engineering can range from minor insecurities to obtaining state secrets[448].

A striking illustration is the 2010 Stuxnet attack. Targeting centrifuges in an Iranian nuclear facility, an unknown attacker reportedly used spear phishing emails to trick an employee into running infected software[449]. Allowing malicious software (malware) to be introduced, Stuxnet illustrates how a non-malicious insider can cause significant damage whilst being unaware that they were

[445] Media reports confirmed that in 2008 the US DoD lost a CD containing the personal details of 207,000 military reservists. In 2008 media reports confirm that the UK MOD lost a device containing the personal details of 600,000 applicants to the UK Armed Forces and the bank details of a further 3,500 Serving Personnel.

Bloxham, "History of Recent Data Blunders by Government".

B. Krebs to Krebs on Security 31 May 2010, https://krebsonsecurity.com/2010/05/stolen-laptop-exposes-personal-data-on-207000-army-reservists/.

S. Hilley, "Uk Ministry of Defence Cracks Down on Ut Security after Theft of Laptop'", *Computer Fraud and Security,* 3 (2008): 2.

[446] Monica Witt was according to media reports recruited by Iranian intelligence and subsequently passed information to Iran that seriously damaged USAF operations. Though it is unknown how Witt was recruited, and the connection with the loss of personal detail is made for illustrative purposes, it indicates that the insider vulnerability is not limited to works of fiction.

BBC, "Ex-Us Air Force Officer Monica Witt Charged with Spying for Iran", *BBC News Online*, 13 February 2019.

A. Goldman and J. E. Barnes, "Air Force Defector to Iran Severely Damaged Us Intelligence Efforts, Ex-Officials Say", *The New York Times*, 15 February 2019.

[447] I. Ghafir, "Security Threats to Critical Infrastructure: The Human Factor", *The Journal of Supercomputing,* (2018): 3.

[448] J.R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies,* 22, no. 3 (2013): 381.

[449] Spear Phishing is defined as the use of an email or electronic communication scam which is targeted at a specific individual, organisation, or business. Often intended to steal data for malicious purposes, hostile actors may also use the method to install malicious software on a target system.

Kaspersky, "What Is Spear Phishing? ", (2020).

complicit[450]. Though not an air power example, it takes little imagination to conclude that if malware can be introduced into a secure nuclear facility via social engineering, it could also be introduced onto an air platform or its ground support systems.

A final but no less serious example is social media. With 62 percent of the UK population reportedly active social media users, insiders who live their lives online could lose clarity as to what is and is not acceptable to share in open forums[451]. Already experienced, media reports confirm that UK military personnel have unwittingly published secret information on social media. Illustrating this point with evidence gained through Freedom of Information (FoI) requests, Farmer reported in 2018 that UK military personnel had via their online personas and social activities 'compromised operations and national security'. This included the publication of secret information on the online networking forum LinkedIn[452]. A salient point through which to conclude this discussion of the non-malicious insiders, it is evident that the potential for air power to experience and be damaged by this cyber vulnerability are extensive.

Malicious Insiders

Similar to non-malicious insiders, this second group also enjoys authorised access to systems. However, unlike the previous group, malicious insiders are distinct in their purposeful use of these privileges to circumnavigate security[453]. Unmanageable through education or repulsed through most technical security measures, some regard them as the most concerning of all cyber vulnerabilities[454].

[450] This summary of Stuxnet is taken from Lindsay. However, it is acknowledged that this is only one of several suggested causes of the incident that have been proffered in academic research and media reporting.
Lindsay, "Stuxnet and the Limits of Cyber Warfare", 381.

[451] Statista.com, "Forecast of Social Network User Numbers in the United Kingdom (Uk) from 2015 to 2022 (in Million Users) ", (2018).

[452] B. Farmer, "Troops Leaked Confidential Data on Twitter and Facebook", *The Telegraph*, , 8 July 2018.

[453] US, "National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat", ed. Department of Homeland Security (National Protection and Programs Directorate Office of Infrastructure Protection, 2013), 3.

[454] The argument for malicious insiders being the most worrying of all cyber vulnerabilities is made by:
N. Catrantzos, "No Dark Corners: Defending against Insider Threats to Critical Infrastructure" (2009), 3.

Like all insiders, those with malicious intent are not unique to technology. Explored by psychologists seeking to understand why an individual would turn against an employer or colleagues, explanations have varied. At one level Cole and Ring argue that all malicious insiders are motivated by one of three factors: money, politics, or personal grievance[455]. Digging deeper, others suggest more prescriptive methods to classify behaviour types[456]. Of these, one overarching theme is the 'Big-Five' personality traits. Though expressed in different variations of the theme, one example is Goldberg's 1993 model which explores whether an individual is more susceptible to being a malicious insider. Developing this question, he divides people into the categories of openness to experience, extraversion, conscientiousness, agreeableness, and neuroticism or emotional stability. In examining this model and critiquing others Goldberg concludes that they do not 'reduce the rich tapestry of personality' but rather offer a high-level description on understanding human motivation[457].

Building on this psychological analysis, the 'Dark Triad' model further focuses the discussion on the question of how the increased use of technology influences the malicious-insider concern. Within this, Paulhus and Williams describe the personality types likely to utilise technology in the pursuit of malicious insider activity. These fall, they argue, into one of three categories: a *machiavellian* tendency who derive behaviour from a manipulative personality, *narcissists* who derive beliefs from a sense of entitlement or superiority and *psychopaths* who derive behaviours from high impulsivity or thrill-seeking[458]. Developing a tangible theory within the often-abstract nature of psychological research, this offers practical value for those seeking to secure digitally driven capabilities such as air power. Specifically, those charged with achieving such security are informed that

[455] E. Cole and S. Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying and Theft* (Massachusetts: Elsevier, 2005), 322.

[456] For discussions on different approaches to classifying, describing, and summarising observable behaviours, see:
John, Hampson, and Goldberg, "The Basic Level in Personality-Trait Hierarchies: Studies of Trait Use and Accessibility in Difference Contexts", 349.

[457] For Goldberg's study, see:
Goldberg, "The Structure of Phenotypic Personality Traits".
For depth on this psychological approach to identifying malicious insiders, see:
US, "Identifying at-Risk Employees: A Behavioural Model for Predicting Potential Insider Threats", ed. Department of Energy (2010), 7.25.

[458] Paulhus and Williams, "The Dark Triad of Personality: Narcissism, Machiavellism and Psychopathy", 557.

to manage human vulnerabilities one must think more broadly than just employing technical security measures[459].

A conclusion supported by other research with a practical focus, early examples include Anderson's 1980 distillation of malicious insiders into three categories[460]. Developed by Salem et al in 2008, they refine their categorisation into two basic distinctions to aide security practitioners: *traitors* who abuse authorised access for malicious intent and *masqueraders* who achieve the same ends by misusing the details of others[461].

Accepting that critics see these models as too simplistic, they still provide identifiable characteristics from which to develop mitigations[462]. The necessity for this is underlined by the fact that despite research repeatedly confirming the importance of the malicious insider vulnerability[463], those charged with protecting technologies remain focused on technical defences. Summarising this issue, Evan et al state that despite the evidence on the importance of the malicious insider vulnerability, there is no evidence of the cyber security industry changing their technically focused practices to address it[464].

In considering this against the realities of delivering air power, we note that with operations relying on people, and a large proportion of these people afforded access to sensitive systems, those responsible for security would be advised to

[459] For discussion on this suggested requirement for activity beyond the purely technical in the defence of networks and systems from the insider vulnerability, see:

M. Massberg, J. Warren, and N.L. Beebe, "The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits", in *48th International Conference on System Sciences* (Hawaii 2015).

[460] Anderson defined malicious insiders as being one of the following groups: *misfeasors* who uses their own privileges, *masquerades* who use the credentials of other authorised users to gain access and *clandestine* users who employ their high degree of technical knowledge to bypass security controls.

J. P. Anderson, "Computer Security Threat Monitoring and Surveillance " in *User Profiling in Intrusion Detection: A Review*, ed. J. Peng, K. Choo, and H. Ashman (Journal of Network and Computer Applications: 2016), 16.

[461] M.B. Salem, S. Hershkop, and S. J. Stolfo, "A Survey of Insider Attack Detection Research," in *Insider Attack and Cyber Security* ed. S.J. Stolgo (Boston: Springer Science and Business Media, 2008).

[462] An example of such criticism is Magklaras and Furnell who assess that models underestimate the complexity of the issue.

G.B. Maglaras and S.M. Furnell, "Insider Threat Prediction Tool: Evaluating the Probability of It Misuse", *Computers and Security,* 21, no. 1 (2001): 64.

[463] Recent white papers which highlight industry acknowledgement of the malicious-insider vulnerability include:

Seuronix, "Insider Threat Survey Report ", (2019).
IBM, "Cost of Insider Threats Report 2020 ", (IBM, 2020).
Egress Software Technologies, "Insider Data Breach Survey ", (2019).

[464] M. Evans et al., "Human Behaviour as an Aspect of Cybersecurity Assurance", *Security and Communications Networks,* 9 (2016): 4669.

reflect on the issue. Though, except for the Monica Witt case cited above, limited information on air power's malicious insiders is openly available, the issues relevance is underlined by the case of Edward Snowdon.

Coming to public attention in 2013, Snowdon downloaded 1,700,000 classified documents whilst working as a contractor for the US National Security Agency (NSA). Leaking a proportion of these to *The Guardian* newspaper, he has been characterised as both a moral whistle-blower and a dangerous insider who caused 'tremendous damage to national security'[465]. Though these contradictions make it unclear which of the 'Dark Triad' categories Snowdon falls into, his actions were undoubtedly a classic example of the malicious-insider vulnerability.

Given that Snowdon achieved this in a highly security conscious organisation, questions on how he did so were bound to be asked. Discussed in *The Guardian*, Snowdon tells how following a short period in the military he worked his way through the Central Intelligence Agency (CIA) as an Information Technology (IT) specialist before becoming a contractor for the NSA[466]. Despite showing signs of being disgruntled with US policy throughout this period, he continued to hold the high-level security clearance that would facilitate his malicious-insider actions.

Examples of this can be found through a review of Snowdon's online activities from as early as 2009. Illustrated via an analysis of his online pseudonym *TheTrueHOOHA,* a trend can be established in which Snowdon regularly posts anti-government messages in open forums. This included on 19 May 2009 public comments on the *Ars Technica* site in which he made claims on the NSA's new surveillance program, suggesting that it was diminishing US freedoms. Furthermore, in the same period the *TheTrueHOOHA* pseudonym was also used

[465] For background on the newspaper articles, see:
M. Kelley, "Nsa: Snowden Stole 1.7 Million Classified Documents and Still Has Access to Most of Them", *Business Insider*, 13 December 2013.
For the moral whistle-blower comment, see:
The-Courage-Foundation, "Who Is Edward Snowdon? ", https://edwardsnowden.com/
For the 'tremendous damage' quote, see:
US, "Review of the Unauthorised Disclosure by Former National Security Agency Contractor Edward Snowden", ed. House of Representatives (2016), i.

[466] Several articles published by *The Guardian* chart this story. For a detailed account, see:
L. Harding, "How Edward Snowdon Went from Loyal Nsa Contractor to Whistle Blower", *The Guardian*, 1 February 2014.

on a *Twitter* account openly connected to Snowdon[467]. Given this, any basic background check of Snowdon should have identified not only the connection between Snowdon and *TheTrueHOOHA* but also his anti-US Government sentiments. If achieved, a review of his security clearance should have followed and, ultimately, his malicious insider activities prevented.

A systematic failure investigated by the US Senate, it was concluded that failings in vetting procedures were ultimately to blame for the Snowdon breach. Offering detailed conclusions, the Senate investigation identified that the body responsible for vetting, the US Government's Office of Personnel Management (OPM), had during the period of Snowdon's employment failed to complete 87 percent of background checks prior to awarding clearances. The OPM had also outsourced 65 percent of all background checks to a civilian contractor, the US Investigation Service (USIS), which was later investigated for fraud. Finally, the OPM had never provided uniform guidelines across government to ensure mandatory baseline requirements were achieved. Collectively, the US Senate concluded, these failings led to Snowdon being allowed the continued access that led to the breach[468].

If these failings had not occurred, it can be concluded that Snowdon's clearances would have been revoked and the malicious-insider vulnerability prevented. Though it is acknowledged that Snowdon is not an air power example, the parallels remain clear. With air forces relying on trusted insiders to deliver operations, there is a constant risk that air force personnel with varying levels of technical abilities or motivations could mirror Snowdon's activities. This is, it is concluded, especially the case if those responsible for personnel security in an air force were to repeat the mistakes made by the OPM.

Notwithstanding the limited examples of this malicious-insider vulnerability, other known events reinforce the above lessons. One notable example is Chelsea

[467] For Snowdon's comments on these online forums, see:
ArsTechnica, 19 May 2009, https://arstechnica.com/civis/viewtopic.php?p=6726096#p6726096
E. Snowdon, "Edward Snowdon / Twitter Account", ed. TheTrueHOOHA (2013).

[468] US, "Snowdon – Preliminary Hearing Transcript", ed. Senate (Senate Committee on Homeland Security and Governmental Affairs, 2013).

Manning. A transgender US soldier formerly known as Bradley Manning, she is known to have downloaded hundreds of thousands of documents from her computer to a Compact Disc (CD) marked 'Lady Gaga' whilst serving with the US Army in Iraq. Having then passed these documents to Wikileaks, the information acquired became known as the Iraq and Afghan War Logs, the Diplomatic Cables, and the Guantanamo Bay files. All releasing potentially damaging details on military and diplomatic operations, the Manning situation is arguably more concerning than that of Snowdon. This is because, unlike Snowdon, Manning did not have a depth of technical expertise. Rather, the simple combination of access and motivation allowed her to cause a very damaging breach of operational information[469]. With this combination easily mirrored in air forces whose personnel are allowed access to the digital systems relied on by today's complex air platforms, it is easy to imagine that a similarly damaging breach could be repeated in the confines of air power.

Reflecting on this, there is a requirement for air forces across both the non-malicious and malicious insider categories to closely examine the issues. Within this, the examples discussed above confirm that if people related cyber vulnerabilities are to be effectively managed, air forces must recognise that non-technical measures are as essential to the assurance of air power as their technical counterparts. Whether such measures are being effectively implemented cannot, however, be known until the next significant breach occurs and proves that they are not.

A final complication of the people layer, it is by virtue of vetting, procedures, and policies that organisations hope to mitigate the vulnerability. However, it is ultimately due to the nature of people that all organisations must rely on the intangible concept of trust. It is when this trust fails within the ranks of an air force or its supporting organisations that the potentially damaging effects of the insider vulnerability will impact the viability of air power.

[469] For depth on the Chelsea Manning breach, see:
H. Alexander, "Who Is Chelsea Manning?", *The Telegraph* 2017.

The Information Layer

The Importance of the Information Layer

Turning to the Information Layer, an environment is identified that is more readily understood by technologists as core to the concept of cyber. Defined by the model as a combination of the connections which exist between network nodes and their logical constructs[470], it can in layman's terms be characterised as the hardware and software which receives inputs, processes data, and stores digital information[471]. Whilst at a basic level this has remained unchanged from the inception of digital technologies, its contemporary manifestation continues to increase in complexity.

When examined in the context of military aviation, the extent of this complexity becomes apparent. As an example, the introduction of NextGen technologies has seen the interconnection of multiple networks aboard a single aircraft[472]. Allowing flight to become increasingly autonomous, innovations have created a fundamental shift away from human-centric to digitally managed operations. Extreme in diversity, such NextGen technologies range from specific developments such as the management of inflight ice protection, through to in-cockpit concepts including Electronic Flight Bags (EFB)[473]. Considered in the broadest of terms, the common factor is how this integration of systems has enhanced the efficiency of aviation[474].

Going further, however, NextGen technologies are also forming CPS that actively monitor and control physical processes previously entrusted to people. With

[470] UK, "Cyber Primer", 7.

[471] The website Techopedia provides a clear definition of computer systems which can be related to the *Cyber Primers* concept of the information layers of the *Layers of Cyberspace* model.
Techopedia, "Computer Systems ", (2018).

[472] It is highlighted that this discussion of NextGen aviation should not be confused with wider industry use of NextGen such as the US Federal Aviation Authority's (FAA) NextGen scheme to modernise US air transportation. Though this touches on the integration of systems to enhance efficiency and safety, its focus is broader and not specifically on aircraft development.
US, "Modernizing Us Air Space: Next Generation Air Transportation".

[473] C. Lawson, "Evaluating Inflight Ice Protection Methods for Application on Next Generation Aircraft", *Journal of Aerospace Engineering and Technology,* 3, no. 3 (2019).
Yeh, Jaworski, and Chase, "Pilot Perceptions on the Integration of Electronic Flight Bag Information in New Flight Deck Designs".

[474] De Cerchio, "Aircraft Systems Cyber Security".

examples including technology making voice communications and visual awareness no longer the primary sources of in-flight information, it is evident that in virtually every aspect digital means have revolutionised modern flight[475].

The result for air power is that digital information has become the 'life blood' of air operations. Recognising this, aviation is presented with a pressing requirement to assure the 'timely, accurate and untampered' nature of digital information which, if compromised, would endanger flight[476]. From a safety perspective, these dangers have been graphically illustrated by the 2019 crashes of the Boeing 737 Max 8 aircraft. Within this, reports regarding one of these disasters, the Lion Air crash in Ethiopia which killed 189 people, provides useful insight. Specifically, the reporting highlights that moments before impact pilots were recorded in the cockpit desperately reading an emergency handbook as they tried to regain control from the aircraft systems[477].

In response, some academic and media analysis has increasingly criticised technology in aviation. For example, Nicas and Wichter's note that 'pilots now spend more time learning automated systems than practising hands-on flying'[478]. Extrapolating this further, it becomes unsurprising that headlines such as *The Guardian's* 'Crash: How Computers are Setting us up for Disaster' have in the last few years continued to highlight public concerns on increasing automation[479].

Despite this, industry commentators unanimously conclude that automation will increase in aviation. Though this runs contrary to the above concerns, it is nonetheless built on a counter-consensus that technology is not to blame for disasters. Rather, as industry website *Robotics and Automation* argues, it is human error that costs human lives[480]. In exploring this, one can conclude that when designed, implemented, and secured properly digital developments in

[475] Discussing the operation of aviation, De Cerchio comments that whereas 'the primary means of obtaining information was through voice, new systems depend on timely, accurate and un-tampered information from mobile, digital networks'. Ibid., 3.
[476] Ibid., 7.
[477] Baker, "The Boeing 737 Max Crashes Have Revived Decades Old Fear About What Happens When Airplane Computers Become More Powerful Than Pilots".
[478] Nicas and Wichter, "A Worry for Some Pilots: Their Hands-on Flying Skills Are Lacking'".
[479] Harford, "Crash: How Computers Are Setting Us up for Disaster".
[480] Staff-Writer, "The Future of Automoation in the Aviation Industry".

aviation are inherently safe. However, it is when digital systems are subject to unforeseen human error, or malicious action to purposefully force their malfunction, that the risk of increasing automation in aviation becomes problematic.

Transposed to this thesis’ exploration of air power’s cyber vulnerabilities, we are reminded of the risk of digital systems being compromised by those with hostile intent. Specifically, with the number of entwined networks and systems processing essential in-flight information now extensive, and every data exchange in and between these, no matter how small, offering a potential for compromise, there is a necessity to ensure high levels of assurance at every step of modern air operations. With any failure to achieve this leading to the potential loss of aircraft and life, identifying and managing information layer vulnerabilities has become a significant challenge for modern air power[481].

Given the scope and complexity of the issue, it is necessary within the confines of this discussion to divide the topic. Specifically, it can be intuitively partitioned into an exploration of direct vulnerabilities to supporting systems and networks, direct vulnerabilities to air platforms and indirect vulnerabilities.

Direct Vulnerabilities to Supporting Systems and Networks

This first category, direct vulnerabilities to supporting systems and networks, are those areas of weakness that could be exploited by hostile actors through a direct attack. Given the breadth of even this sub-division, to effectively illustrate the topic it is necessary to consider examples that highlight the type of challenges air power faces.

An initial example is the exploitation of vulnerabilities within a military’s own User Access Devices (UAD) such as desktop computers, laptops, tablets, and

[481] This characterisation of the vulnerability of digital systems is made by the US OTE Agency.
US, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs: Memorandum for Commander Army Test and Evaluation Command and Air Force Operational Test and Evaluation Centre".

smartphones[482]. An element of networks that are so routinely used that they can often appear benign, UADs must be properly managed and hardened through basic security practices including patching and anti-virus (AV) measures. If this does not occur vulnerabilities can be created which, when exploited, have serious consequences[483].

An issue discussed by Freeberg, he highlights that in the decade following 2003 the Wests adversaries repeatedly achieved direct access to military networks by exploiting UADs[484]. Citing one case specifically, he discusses how in 2008 a US military system in the Middle East was infected by malware through the connection of a Universal Serial Bus (USB) memory stick to a military laptop. Exploiting a basic vulnerability created by a failure to harden the device, in this case not locking down access to the laptops USB ports, the impact due to the local networks onward connectivity was not localised[485]. Rather, reports indicated that the malware infected Department of Defence (DoD) servers in the US causing far greater disruption than the simple loss of a single laptop or a local network[486].

Not an aviation specific example, the scenario still illustrates how in a military environment even the most basic information layer vulnerability can, when exploited, cause widespread impact. With air power systems including platforms now connected to core networks, a similar exploitation when targeted effectively could have a devastating impact on an air force's operational delivery[487].

Considering a further direct example, the compromise of information layer vulnerabilities does not need to target military systems to have significant

[482] UAD's provide the hardware through which users interact with data and applications. Examples include, but are not limited to, desktop computers, laptops, tablets, and smartphones. For a definition of end user devices, see:
UK, "Government End User Device Strategy", (HM Government 2011), 3.

[483] Hardening refers to a suite of basic security practices that should be used on all systems to prevent breaches and incidents. These include, but are not exhaustively, software patches, AV and disabling unnecessary USB ports. For depth, see:
Techopedia, "Hardening ", (2020).

[484] S. Freeberg, "Top Official Admits F-35 Stealth Fighter Secrets Stolen", *Breaking Defence*, 20 June 2013.

[485] For a discussion of the risks posed by USB ports to systems and networks, see:
ComputerSecrity.com, "White Paper: Approaches to Usb Security ", (2020).

[486] C. Magee, "Awaiting the Cyber 9/11" (USMC University, 2012).

[487] Alongside the rise in global connectivity afforded by the internet, the vulnerabilities of physically connected networks across extensive locations have been at the forefront of IT security concerns. For depth on this issue, see:
A. Simmonds, P. Sandilands, and L. van Ekert, "An Ontology for Network Security Attacks", in *Asian Applied Computing Conference* (2004).

operational impact. For example, media reports in 2013 confirmed that the systems of Lockheed-Martin, the prime-contractor for the F-35 aircraft, were compromised[488]. Reportedly leading to sensitive information relating to the aircraft being stolen by state-sponsored PRC hackers[489], the incident did not directly affect air operations. However, it is suspected to have contributed to the development of the PRC's J-20 stealth fighter aircraft[490].

Allowing in this example the PRC to take big steps forward in aircraft development, this exploitation reduced the West's expected relative technological advantage. A claim proven through the publication of the Snowdon leaks in 2013, it was reported that in 2007 PRC state-sponsored hackers, in events codenamed the *Byzantine Hades* hacks by the US, caused serious breaches in DoD systems. Including a catalogue of over 30,000 incidents and 500 significant intrusions, the reports show that at least 1,600 DoD computers and 600,000 user accounts were compromised. Allowing 50 terabytes of data to be taken, an amount equal to 5 Libraries of Congress, the stolen details are reported to have included the aforementioned information on the F-35. With subsequent media analysis of the J-20 showing striking similarities with the F-35, we are offered compelling evidence that the *Byzantine Hades* hacks allowed the PRC advances in technology. It can therefore be concluded that this form of cyber vulnerability is arguably more concerning than any immediate but short-term impact[491].

Reflecting on this one might expect that breaches on the scale of the *Byzantine Hades* hacks are now managed and mitigated to a point at which they could not be repeated. However, reporting which first emerged in December 2020 relating

[488] The F-35 is an advanced fighter produced by Lockheed-Martin for nations including the US and UK.
LockheedMartin, "About the F-35: The Multi-Variant, Multirole 5th Generation Fighter".

[489] Media reports following the compromise of Lockheed-Martin systems initially identified the potential impact of the loss but failed to identify the attacker. Following the Edward Snowdon leaks, however, it was identified that US intelligence had credible evidence to suggest that the attack come from PRC state sponsored hackers. For depth, see:
Freeberg, "Top Official Admits F-35 Stealth Fighter Secrets Stolen".
J. Applebaum, "Nsa Preps America for Future Battle", *Das Spiegel* 2015.

[490] The J-20 is an advanced fighter produced by the Chengdu Aircraft Industry Group which entered service with the Chinese People's Liberation Army Air Force (PLAAF) in 2017.
Roblin, "Can China's Chengdu J-20 Stealth Fighter Win against America's F-35 or F-22".

[491] For depth on the background, impact and assessment of the *Byzantine Hades* hacks, see:
StaffWriter, "Hacked: How China Stole Us Technology for Its J-20 Stealth Fighter", ibid., 10 July ; ibid.
F.S. Gady, "New Snowdon Documents Reveal Chinese Behind F-35 Hack", *The Diplomat*, 27 January 2015.

to exploited vulnerabilities in software provided by the US company SolarWinds showed that this is not the case.

A major provider of network management software, SolarWinds publicises their products as allowing clients to oversee and remotely manage complex enterprise-wide networks[492]. Though powerful, the intrusive nature of such software allows authorised users virtually unfettered access to an organisation's networks, systems, and information. Therefore, when a hostile actor believed to be linked to the Russian state compromised SolarWind's Orion software by installing a 'backdoor' in a routine update, extensive covert access to the systems of all those using Orion was created[493].

With this vulnerability in place for what is believed to be over a year, and the SolarWind client list running to over 18,000 public and private sector organisations, the potential impact of this breach was huge. Going further, it is notable that in the US alone the SolarWinds software was used by the US Government departments of Defense, Commerce, Energy, Homeland Security, State, the Treasury and Health[494]. Based on this, we find a breach that not only matched but eclipsed the potential damage of the *Byzantine Hades* hacks. Whilst Skinglsey tempers this statement in her argument that no damage to systems, networks or infrastructure is known to have been done, the comparative advantage the hostile actor, thought to be Russia, is likely to have achieved via the SolarWinds breach is arguably beyond calculation[495].

Taken collectively, the above discussion illustrates the breadth of vulnerabilities that must be considered when exploring the information layer. Whilst the examples offered are few, and not all are related specifically to air power, the

[492] SolarWinds, "Leader in Network Management Software and Monitoring Tools", (2021).

[493] US, "Joint Statement by the Federal Bureau of Investigation (Fbi)", ed. the Office of the Director of National Intelligence (ODNI) and the National Security Agency (NSA) Cybersecurity and Infrastructure Security Agency (CISA) (2021).

[494] M. Korolov, "The List of Known Solarwinds Breach Victims Grows, as Do Attack Vectors", (Data Centre Knowledge, 2021).

[495] For Skingsley's comments, see:
J. Skinglsey, "The Solarwinds Hack: A Valuable Lesson for Cybersecurity", *Chatham House,* (2021).
For detail on the SolarWinds breach, see:
BBC, "Solarwinds: Hacked Firm Issues Urgent Security Fix", *BBC News* 2020.
SolarWinds, "Cert Advisory: Vulnerability Report", (2021).

lessons for air forces are no less stark. Specifically, to maintain the viability of air power the systems and networks that support it must be relied on. If an adversary can disrupt operations by attacking these systems and networks, or gain enhanced advantage through breaching, the aims of the first cause will not be met and the desire to survive and thrive will be lost. Therefore, though a single breach might be manageable, the depth and breadth of the *Byzantine Hades* and SolarWinds breaches if directed against air power would undermine the viability of the capability. Given this, the challenge for those charged with identifying and managing direct vulnerabilities to networks and systems becomes stark.

Direct Vulnerabilities to Air Platforms

Though the above direct vulnerabilities to the systems and networks defence relies on are significant, perhaps the most concerning topic for this discussion are the direct vulnerabilities within the air platforms themselves. To explore this, there is value in taking two specific case studies from which the level of vulnerabilities can be ascertained: UAVs and the US led coalitions F-35.

Considering the first, UAVs, proponents argue that their increasingly autonomous operations represent the future of air power[496]. Allowing through the removal of the human pilot air power to escape traditional limitations of reach and duration, Air Chief Marshall Sir Mike Wigston, Chief of the Air Staff for the RAF from 2019 to 2023, predicted that by 2040 80 percent of aircraft will be unmanned[497]. Ranging from swarming UAVs able to mimic the behaviour of nature and simultaneously attack a target from all sides to more conventional combat drones able to replace traditional fighter-bombers, the shift arguably represents the greatest change in the air domain since its inception[498]. With the US military also having increased investment in the research and production of UAVs to $4.2 billion by 2012, there can be no doubt that these autonomous platforms will in

[496] Hartmann and Steup, "The Vulnerability of Uavs to Cyber-Attacks; an Approach to the Risk Assessment", 1.
[497] M. Wigston, "Trenchard Memorial Lecture", *RUSI* (2021).
[498] For detail on swarming and combat UAVs, see:
J. Arquilla and D. Ronfeldt, *Swarming and the Future of Military Conflict* (Santa Monica: RAND, 2000).
F. Grimal and J. Sundram, "Combat Drones: Hives, Swarms and Autonomous Action", *Journal of Conflict and Security Law,* 23, no. 1 (2018).
I. Lachow, "The Upside and Downside of Swarming Drones", *Bulletin of the Atomic Scientists,* 73, no. 2 (2017).

short order dominate conflict, possibly much sooner than Wigston's prediction of 2040[499].

Whilst through this UAVs will increase the utility of air power and the level to which states rely on it, Hartmann highlights that due to their nature as complex systems they are exposed to compromise[500]. With this concern enhancing in line with their expanded use, digital attacks targeted against their vulnerabilities have increased over the last two decades. For example, in 2009 investigations identified that the unencrypted video feed from a US drone operating in the Gulf Region had been compromised by an unconfirmed terrorist group. Reported to have used the commercially available SkyGrabber software, a low-cost Russian capability that intercepts unencrypted satellite communications, it allowed the group to see and record live video feeds[501]. With such feeds often identifying the location and movement of friendly forces, the exploitation of this vulnerability could in the wrong hands create a credible risk to life.

Looking beyond this single example and examining how similar vulnerabilities might also threaten UAVs in operation, the topic of encrypted data links demands further consideration. With their use by UAVs both longstanding and widely known, it is unsurprising that the SkyGrabber example is not the only reported exploitation. In a second, a US Sentinel UAV was in 2011 captured by Iran. Confirmed in a press conference by President Obama, analysts have suggested that it was likely achieved through vulnerabilities in the UAVs navigation system[502]. Specifically, Humphrey explains that Iran probably used Global Positioning Satellite (GPS) spoofing to exploit the fact that GPS has no robust encryption or built-in protection against counterfeiting. This vulnerability allowed

[499] Hartmann and Steup, "The Vulnerability of Uavs to Cyber-Attacks; an Approach to the Risk Assessment", 1.
[500] Ibid.
[501] For detail on SkyGrabber, see:
Software.Informet, "Skygrabber 2.6 ", (2021).
For detail on the assessed use of SkyGrabber against US UAVs, see:
C. Arthur, "Skygrabber: The $26 Software Used by Insurgents to Hack into Us Drones", *The Guardian*, 17 December 2009.
[502] R. Gladstone, "Iran Is Asked to Return Us Drone'", *New York Times*, 12 December 2011.
Hartmann and Steup, "The Vulnerability of Uavs to Cyber-Attacks; an Approach to the Risk Assessment", 1.

Iran to hijack the GPS signal controlling the UAV and, as a result, redirected it to land on an Iranian airfield[503].

In reflecting on these examples, and whilst acknowledging that those vulnerabilities explored are relatively niche, a picture is presented in which UAVs offer both considerable utility but also increased risk. If such concerns are not effectively managed, the end state could, if Wigston's prediction comes to fruition, mean that states who rely on UAVs are even more exposed to cyber risk than the previous Chapter suggests. If so, one might conclude that states should be advised in the future to choose manned rather than unmanned options so that the vulnerabilities can be mitigated. Though logical, a review of the vulnerabilities associated with the F-35 show this argument if taken in isolation to be flawed.

Immensely complex, the F-35 is produced by defence contractor Lockheed-Martin for the US, 9 international partners and 6 other purchasers[504]. Entering service with the US in 2015, the F-35 has since that date been deployed on combat operations. Furthermore, a review of the procurement strategies of those involved in the programme shows that for some states including the UK the F-35 will become a mainstay in their air power capability[505].

Though in support of this intent the F-35 is claimed by Lockheed-Martin to be the 'most lethal, survivable and connected fighter aircraft in the world', a claim supported by industry commentators, it is also one of the most digitally reliant[506]. Taking in Lockheed-Martin's own estimation 'more than steel, advanced electronics and engine thrust to make [it]…take flight', the platform is unable to operate without its systems and networks[507]. Specifically, amongst the many

[503] T. Humphrey, "Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil Gps Spoofing", ed. Investigations Submitted to the Subcommittee on Oversight, and Management of the House Committee on Homeland Security (US Congress 2012), 1.
[504] Lockheed-Martin, "The Global F-35 Enterprise ", (2021).
[505] G. Allison, "F-35b Enters Operational Service", *UK Defence Journal*, no. 3 August (2015).
P. Suciu, "Is the Uk Considering Cutting Its Order for the F-35?", *The National Interest*, 13 March 2021.
[506] For the quote, see:
Lockheed-Martin, "The Most Advanced Fighter Jet in the World ", (2021).
For industry comment on the F-35 which supports Lockheed-Martin's claims, see:
L. Shiner, "F-35: What the Pilots Say", *Air and Space Magazine*, April 2019.
G. Allison, "What's So Good About the F-35 Anyway?", *UK Defence Journal,* (2019).
[507] Lockheed-Martin, "Autonomic Logistics Information System (Alis) ", (2018).

NextGen elements it relies on, the Autonomic Logistics Information System (ALIS) has arguably been the most pivotal.

Whilst ALIS is scheduled to be replaced by the reportedly more stable Operational Data Integrated Network (ODIN), the issues experience with ALIS throughout its development and use illustrate the underlying vulnerabilities that can be experienced by advanced air platforms[508]. Designed to provide 'a comprehensive logistic support environment', ALIS like other support systems delivers an array of advanced services[509]. However, going further than most, ALIS and its ODIN replacement offer everything from Prognostics and Health Management (PHM), through to enhance aircraft safety and efficiency, automated technical support, and digital links not only between aircraft but back to Lockheed-Martin[510]. When viewed collectively, the chief F-35 test pilot, Alan Norman, compared ALIS to R2-D2. Referring to the *Star Wars* droid that helped Luke Skywalker fly his X-Wing, Norman asserted that ALIS is the 'ultimate in human-machine interaction'[511].

With this level of integration increasing alongside the development of ALIS, the system by 2017 had, in Brissett's estimation, achieved for the first time a fully integrated platform spanning every element of the aircraft 'from tip to tail'[512]. Making it the 'single, secure information environment…for all elements of F-35 operations', one could conclude that it became the keystone of a capability that itself was planned to become central to the defence of its partner nations. Given this, it should have been expected that serious questions would be asked on whether ALIS had digital vulnerabilities that might endanger this role. Summing up the importance of such questions, Bender commented that if an adversary compromised ALIS 'they've essentially defeated the plane…[without] firing a bullet' and could, in turn, undermine the entire strategic intent of the state's operating it[513].

[508] G. Reim, "First Lockheed Martin F-35s Loaded with Odin Hardware'", *Flight Global*, 9 October 2020.
[509] S. Henley et al., "Autonomic Logistics - the Support Concept for the 21st Century'", in *Aerospace Conference* (2000), 417.
[510] Ibid.
[511] Norman, "Can the Us Military's New Jet Fighter Be Hacked?."
[512] W. Brissett, "Alis 2.02 Ready to Go", *Air Force Magazine*, 28 March 2017.
[513] J. Bender, "The New F-35 Fighter Jet Can Be Taken Down without a Bullet Ever Being Fired", *Business Insider*, 18 February 2014.

In examining a potential answer to these questions on ALIS, a surprising amount of concerning detail has been openly published by the US. For example, as early as 2012 it was reported that USN penetration testers exploited Lockheed-Martin's failure to separate classified and unclassified data streams[514]. Although a workaround to create an 'air gap' allowed the continued development of ALIS, this early event pointed towards revelations to come[515].

With reporting next surfacing in 2015, Lockheed-Martin under pressure from previous failures, acknowledged that there had been a significant number of sophisticated attacks aimed at its networks[516]. Levelling the blame at unnamed states it was increasingly evident that hostile-actors were intent on identifying and compromising vulnerabilities associated with the F-35. Despite this, 2015 also saw further deep-seated vulnerabilities in ALIS being identified. A significant event which illustrates this was US Marine Corp (USMC) Operational Test One (OT-1). Held in May 2015, OT-1 saw seven F-35s embarked on the aircraft carrier the United States Ship (USS) Wasp[517]. Though the USMC used the OT-1 to 'triumphantly declare' its variant of the F-35 combat ready, such fanfare hid major technical failings which created concerning vulnerabilities[518].

Summarised in a US OTE memorandum, it was reported that the technical limitations of ALIS led, during OT-1, to the USMC taking 'extraordinary measures to keep the planes flying'[519]. Of note, to operate effectively and support F-35 operations ALIS must achieve routine data transfer between the system nodes: the Squadron Operating Units (SOU) that was aboard the USS Wasp and the core Autonomic Logistics Operating Unit (ALOU) hosted by Lockheed-Martin[520]. However, failures in the datalinks forced the support team to return from the USS

[514] A. Shalal-Esa, "Lockheed's F-35 Logistics System Revolutionary but Risky", *Reuters*, 16 November 2012.
[515] D. Majumdar, "Usmc Finds Workaround for Cyber-Vulnerability of F-35 Logistics System", *Flight Global*, 21 November 2012.
[516] Shalal-Esa, "Lockheed's F-35 Logistics System Revolutionary but Risky".
[517] US, "Observations on the Marine Corps F-35b Demonstration on Uss Wasp: Memorandum for under Secretary of Defense for Acquisition, Technology and Logistics", ed. Operational Test and Evaluation (2015), 1.
[518] D. Grazier and M. Smithburger, "Pentagon Testing Office Calls Foul on F-35 Operational Testing", in *Project on Government Oversight* (Centre for Defence Information, 2015).
[519] Ibid.
[520] US, "Observations on the Marine Corps F-35b Demonstration on Uss Wasp: Memorandum for under Secretary of Defense for Acquisition, Technology and Logistics", 1.

Wasp, travel off base to a location with commercial wi-fi and download the aircraft files. From there, the team burnt the files to CDs and manually uploaded the data onto the USS Wasp SOU. An immense breach of security operating procedures for any secure military system, the action introduced numerous vulnerabilities at every stage of data transfer. However, with no other way to circumnavigate the failing of ALIS, the risk was taken to ensure operational delivery[521].

Reflecting on this, the lessons for air power becoming reliant on air platforms that are themselves reliant on digital information becomes obvious. Whilst in this controlled training scenario the risks taken might have been acceptable, the situation would have been entirely different in combat where hostile actors are more keenly focused on finding vulnerabilities. In such circumstances, an exploited vulnerability found within this process of data transfer would not only have caused reputational damage but may have also cost lives.

In exploring how such a scenario might play out if the above vulnerabilities were compromised, it is informative to consider these ALIS related concerns in other contexts. For example, 2014 reporting suggested that ALIS is capable of 'disallowing the human pilot' from controlling the F-35 if the system senses a problem[522]. A safety measure designed to prevent pilots exceeding their capabilities or continuing to operate with an unidentified malfunction, it is plausible that if malware were introduced onto ALIS an adversary could trigger such an action, grounding an entire fleet or even causing an aircraft to crash[523]. With Lockheed-Martin reacting to such claims by stating 'that they are working hard to remove vulnerabilities', it would be expected that the above concerns were quickly managed[524].

However, subsequent reporting continued to confirm that Lockheed-Martin was failing to remove known vulnerabilities from ALIS. For example, in 2016 the US Joint Program Office (JPO) refused to proceed with scheduled cyber security

[521] Ibid.
[522] Cyberwarzone, "New F-35 Jet Is Vulnerable to Cyber Attack", *Cyber-Security News*, 31 May 2014.
[523] Ibid.
[524] D. Grazier, "F-35 Officials Prove Need for Cyber Testing by Cancelling One", in *Project on Government Oversight* (Centre for Defence Information, 2015).

tests because of concerns that the use of realistic 'hacker tools' could easily compromise and damage the system which was not prepared for that level of intrusion. If this occurred, it was concluded, approximately 100 aircraft already in service might be grounded[525]. Unwilling to take this risk on a system already known to be flawed, the US decided to cease all planned testing. As might be expected, this raised widespread concerns with media reports at the time asking 'obvious and disturbing questions about what could happen in combat'[526].

Moving forward to 2017, these issues remained unresolved. Confirmed by the US OTE annual report for financial year 2017, it was noted that some of the previously reported ALIS vulnerabilities 'still had not been remedied'[527]. Though it is recognised that with the proposed rollout of ODIN these ALIS issues should be resolved, the underlying concern remains prevalent to not only F-35 but all modern air platforms.

Specifically, if air power is to be entirely reliant on supporting information systems, then the operations of those information systems are as important as whether the air platform can itself get airborne. If they fail due to known vulnerabilities, then confidence in air power will be lost unless quick mitigation can be provided. With the F-35 showing that even after 6 years of operational service this end state had not been achieved on what is a 'flagship' project, then perhaps the systems of all modern air power, whether manned or unmanned, hold too many vulnerabilities to be viable. If this is the case, the reliance explored in the previous Chapter has the potential to be exposed, and the relative position of those states who rely on it placed at risk.

Indirect Vulnerabilities

Though the above direct vulnerabilities are the most obvious issues within the information layer, they are potentially not the greatest long-term concerns.

[525] Ibid.
[526] Ibid.
[527] US, "F-35 Joint Strike Fighter Fy 17 Department of Defence Projects ", ed. Operational Test and Evaluation (2018), 33.

Alternatively, it may be an adversary's ability to indirectly create information layer vulnerabilities by compromising components in the supply chain that are the most impactful. An assertion made by the UK's Computer Emergency Response Team (CERT-UK), it is, they conclude, the 'weak links' in a supply chain and not necessarily the military themselves that are the most likely avenues through which adversaries will compromise air power. Specifically, they conclude, it is the potential to place unseen malware on components before they are even delivered for operational use that should be most closely considered[528].

An example of where this issue offers a particularly heightened risk is that of counterfeit computer chips. Electronic circuitry embedded in silicon, computer chips provide the core component of all modern technology[529]. Virtually impossible to identify once introduced into the supply chain, a US Congressional investigation concluded that such counterfeits are not only assessed as increasingly prevalent but present a far greater risk of failure than genuine versions[530]. Whilst a concern for all arms of the military, this issue is particularly troubling for aviation. This is because, to avoid catastrophic failure in flight, air platforms demand exacting levels of reliability from every component on an aircraft. If a counterfeit chip were to fail, so could the entire air platform.

Although it is difficult to discern the scale of this supply chain vulnerability, media reports claim that counterfeit chips have already been introduced into military supply chains. An example which illustrates this was the sale by a US company of PRC produced counterfeit chips to the US military in 2010[531]. Repeated in 2013 with counterfeit chips of an unknown origin being sold to the US for use in its' nuclear submarine fleet[532], it can be surmised that if these examples have reached the public domain, then they are likely to be the 'tip of the iceberg' with the true scope yet to be realised.

[528] CERT-UK, "Cyber Risks in the Supply Chain", ed. CERT-UK, White Paper (2015), 4.
[529] TechTerms, "Computer Chip", in *Hardware Terms* (2018).
[530] Congressional Committee on the Armed Services, "The Committee's Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain", ed. US Congress (2011), 36.
[531] R. McMillan, "Woman Helped Sell Fake Chips to Us Military", *PC World News*, 23 November 2010.
[532] Boyson, "Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical It Systems".

This issue is, however, arguably set to get worse. With the cost of genuine chips rising by 20 percent in 2018 combining with global reductions in Defence spending as a proportion of Gross Domestic Product (GPD) and a reinvigoration of governments questioning contractor's profit margins, there is an increasing motivation for suppliers to cut costs[533]. With such pressure routinely pushed down from prime contractors to the type of sub-contractors who produce and deliver computer chips, it is logical that elements of the supply chain will look to protect their own profits by sourcing cheaper alternatives.

Taking Boeing who are supplying UK Defence with the P-8 Maritime Patrol Aircraft as an example, reports indicate that the company has been actively squeezing their suppliers to cut prices and maintain their profit margins[534]. With *The Financial Times* stating that this represents standard practice across most of UK Defence's prime contractors, the result will be sub-contractors seeking ways to cut cost[535]. Contrasted against the above statement on the increase in price of genuine chips, the result will logically be more counterfeits being introduced into the supply chain. With these then likely to reach aircraft systems, the impact for air power will go unseen until a failure in flight occurs. At that point, the gravity of the situation might be realised but it will be too late to effectively manage the vulnerability.

Whilst safety is of concern, the issue of supply chains allowing information layer vulnerabilities to be indirectly created has an even more sinister aspect.

[533] For rises in the cost of chips, see:
M. Wilson, "Silicon Wafer Makers Plan 20% Increase in Price in 2018", *Kit Guru.net* (2018).
For reporting on reductions in spending as a proportion of GDP, see:
World-Bank, "Military Expenditure (% of Gpd) – United Kingdom (2019)", https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS.
UK, "Finance and Economics Annual Statistical Bulletin: International Defence 2019 ", ed. Ministry of Defence (2019).
J. Lewis, "Defence Spending Continues to Decline", ed. UK Parliament (HM Government 2019).
For reporting and discussion on Governments reviewing and pushing down supply chain costs, see:
J. Gould, "A Company Made a 4.436% Profit on a Cheap Part Sold to the Pentagon", *Defence News*, 15 May 2019.
US, "Dod Inspector General Report on Excessive Profits by Transdigm Group, Inc'", ed. Department of Defence (Inspector General 2019).
UK, "Government Outsourcing: What Has Worked and What Needs Reform? ", ed. Institute for Government (HM Government 2019), 14.

[534] J. Johnson and P. Robison, "Boeing Is Killing It by Squeezing Its Suppliers", *Bloomberg Businessweek,* (2018).

[535] J. Fontanella-Kahn and S. Pfeifer, "United Technologies-Raytheon Deal Creates Aerospace Powerhouse", *Financial Times*, 10 June 2019.

Specifically, there is a risk that hostile actors could purposefully introduce malware onto the components which form part of military aircraft.

Though not aviation specific, a military example of this is identified in reports of malware being found on hard drives delivered to the US by Seagate, a US technology company. Produced for Seagate in Thailand, the hard drives contained 'report-back' software which directed all information saved on them to be sent to a PRC Internet Protocol (IP) address as soon as an internet connection was made[536]. Whilst media reports do not confirm whether the vulnerability was exploited, it nonetheless identifies the potential for devastating losses of sensitive data to occur through an indirect information layer vulnerability.

This Seagate example also points towards the global breadth and depth of this issue. For example, as Borg reported in 2010, media investigations have confirmed that the US NSA has itself infected hard disks from companies including Seagate with spyware designed to gather information from its adversaries. Targeting states including Russia, Pakistan, Afghanistan and the PRC, this development shows how diverse global supply chains can be compromised by numerous different parties for their own purposes. With it further illustrating how the practice could now be considered common across all states with the capability to do so, one can conclude that, on balance, a large proportion of those who have used the method have also been targeted by it. Based on this, it becomes a matter of time before an adversary uses this information layer vulnerability to negatively affect other states' air power[537].

A final but even more impactful example is the introduction of malware onto aircraft systems through the supply chain. One example is logic bombs[538]. Designed to be hidden and dormant within a system until triggered by an activity

[536] J. Menn, "Russian Researchers Expose Breakthrough Us Spying Program", *Reuters*, 16 February 2015.

[537] S. Borg, "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework", *The Internet Alliance,* (2010): 1.
D. Pauli, "Your Hard Drives Were Riddled with Nsa Spyware for Years'", *The Register,* (2015).

[538] Logic bombs are a type of programming code that lies inactive until a particular piece of program logic or a specific event activates it. Common activators have been reported to include a date or time or a certain message from the programmer. In some circumstances the code can be activated when something does not happen. Though unlike other malware a logic bomb cannot replicate itself and infect other systems, it can have significant impact on the system that has been infected by it.
H. R. Zeidanloo et al., "All About Malwares (Malicious Codes)", *Security and Management* (2010): 345.

or pre-defined event, industry analysts have suggested that they could be used to target the military[539]. A potential explored by Borg, he argues that if correctly targeted a hostile actor could use a logic bomb to shut down the overarching information system of an aircraft or, in a worst-case scenario, turn the aircraft against those operating it[540].

Reflecting on these indirect means it is clear, as it was with direct vulnerabilities, that the scope is extensive. With such vulnerabilities routinely extending outside of governmental and military control into the sphere of civilian suppliers, the challenge of identifying and managing them continues to grow in not only complexity but urgency. Given this, it becomes in conclusion not a matter of 'if' information layer vulnerabilities will negatively impact air power but 'when', and to 'what extent'?

Over Exaggeration or Prudent Concern?

In responding to this question, it can be asserted that though the information layer vulnerabilities explored above could, if exploited, have devastating impact on air power, the risk they present might be characterised as over exaggerated. Though academics such as Schwartau infamously warned in 1991 that a 'Cyber Pearl Harbour' will cripple military and civilian capabilities, the reality 3 decades later is that such events have not materialised[541].

With the world continuing to be a hostile and unstable environment, one might therefore conclude that this proves that the information layer vulnerabilities explored above offer too apocalyptic a scenario. Further, with the information layer now protected by proven technical defences, the risk of a 'Cyber Pearl Harbour' can be argued to have passed[542].

[539] S. Northcutt, "Logic Bombs, Trojan Horses and Trap Doors", *Sans Technology Institute,* (2018).

[540] Borg, "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework", 1.

[541] W. Schwartau, "Hearing before the Subcommittee on Technology and Competitiveness on Computer Security", (US Congress, 1991).

[542] Within military and governmental cyber activities, technical defences of systems are usually labelled as Computer Network Defence (CND). Sitting under the overarching category of Computer Network Operations (CNO) (which also includes the offensive aspect of Computer Network Attack (CNA)), CND is commonly accepted to include an array of technical means to protect systems and networks from external intrusion and attack. Collectively, when delivered in a coordinated manner, CND provides proven technical measures which assure that information layer vulnerabilities are

However, even if one might hope this to be true, the reality is that information layer vulnerabilities which sit at the core of digital delivery will, if exploited, have a devastating impact on air power. Furthermore, the examples discussed above illustrate that in some forms they have already occurred and, in others, have the potential to be dormant but activated at a strategically decisive moment. It is therefore concluded that expecting the worst by approaching information layer vulnerabilities with prudent concern is the only advisable path to assuring the continued viability of air power.

The Real Layer

Critical Infrastructure and Aviation

The final aspect in this discussion of cyber vulnerabilities is air power's real layer which can be subdivided into two distinct elements: the geographic aspect, or the actual location of equipment which makes up a system or network, and the physical aspect, or the components that are present in that geographic location[543]. Focusing on the hardware, software and infrastructure which represent the manifestations of cyber, it is identifying which assets support the operational delivery of air power, and their potential vulnerabilities, that form the focus of considerations within this layer.

Whilst the layer includes in its above definition hardware and software, the most tangible element when exploring its' cyber vulnerabilities are the physical infrastructures that house both. When considered from this perspective, the challenges experienced by air power are intuitively examined through the lens of critical infrastructure.

identified and managed. A well-trodden path, it should be expected that government and military organisations will employ strong CND methods.

P. Cornish, R. Hughes, and D. Livingstone, "Cyberspace and the National Security of the United Kingdom: Threats and Responses", *A Chatham House Report,* (2009): 6.

UK, "Cyber Essentials: Technical Controls ", (National Cyber Security Centre, 2020).

[543] "Cyber Primer", 5.

A term most simply defined as those elements 'necessary for an organisation to function', critical infrastructure in the context of air power are any assets which, if lost or compromised, would prevent the effective delivery of air platforms[544]. Though obvious examples may include runways and ATC, the reality is that the demand for infrastructure in aviation runs much deeper.

Divided by UK air power doctrine into three distinct sub-sections of operations support, logistics and administration, air power when compared to the other arms of the military is uniquely reliant on secure operating bases and its associated critical infrastructure. Though in making this statement it is recognised that the other military domains of land and maritime require basing to operate effectively, neither are as dependent on it as air power. For example, whereas land forces can operate in austere conditions with resupply from a variety of sources, and maritime forces can operate at sea for prolonged periods with resupply via other vessels, the limited duration of air platforms demands their frequent return to secure bases. Further, in delivering this base environment there is a plethora of essential infrastructure such as fuels, power and engineering that must be maintained. If they are not, air power will cease to operate.

Given this, there is a clear imperative in the projection of air power to assure the real layer. To do so in this digitally enabled world, an air force must not only provide physical protection to infrastructure but also understand and manage the cyber vulnerabilities. It is this aspect of the real layer that the following sections will explore.

Digital Enablement and Real Layer Vulnerabilities

Though protecting air bases has been a challenge throughout the history of military aviation, the issue has become increasingly demanding with the digital enablement of physical infrastructure. Following trends across all modern industries, air operations and the infrastructure which supports it have become

[544] The definition is provided in:
"Critical National Infrastructure ", ed. Centre for the Protection of National Infrastructure (2018).

intrinsically linked to what Cornish et al defines as the 'interconnected and knowledge-based economy'[545]. Mirroring the development of NextGen aircraft, complex CPS are now routinely relied on to deliver effective infrastructure[546].

Creating a reality in which digital networks form the 'backbone of critical infrastructure'[547], organisations from across numerous sectors including aviation acknowledge that a cyber breach targeting infrastructure could have a significant impact on operational delivery[548]. An example of such an event was the 2015 cyber attack on the Ukrainian power grid.

First reported in the media on 24 December 2015, this synchronised attack by Russian security services was built on extensive reconnaissance of vulnerabilities intrinsic to the real layer of the targeted networks. With the attack delivered through phishing emails to the employees of the power company, malware designed to exploit identified vulnerabilities was introduced onto the infrastructure's software. The impact was major power outages that disrupted over 50 sub-stations and led to more than 220,000 consumers losing power. Responding to the events, Ukraine was faced with an unprecedented real layer impact of having to shift from an automated power grid to manual operations in each of the affected sub-stations[549].

This attack shows how cyber vulnerabilities in the real layer can, when exploited, have tangible impact. Given this, and the widespread impact that occurred, one would assume that organisations have learnt and, in turn, actively sought to remove cyber vulnerabilities from critical infrastructures. However, the cyber

[545] Cornish et al., "Cyber Security and the Uk's Critical National Infrastructure", vii.

[546] For a discussion of how the 'lifeline of our modern society' is provided by critical infrastructures which are dependent on CPS to achieve reliable secure operations, see:

Chee-Wooi, Manimanran, and C., "Cybersecurity for Critical Infrastructures: Attack and Defense Modelling".

[547] Ibid.

[548] For example, a survey of security professionals across 6 countries (including the UK) by the Ponemon Institute found that 90 percent of organisations had been targeted by at least one successful cyber attack which targeted infrastructure. Including industries such as energy, health and transport, the BBC quotes 'experts' who reviewed the results as calling it a 'wake-up call for industry'.

Ponemon-Institute, "Study on the Cyber Resilient Organisation ", (2019).

D. Simmons, "Cyber-Attacks 'Damage' National Infrastructure", *BBC News* 5 April 2019.

[549] The cyber incident in Ukraine in 2015 was first reported in the media via Ukrainian news outlet TCH on 24 December 2015. For depth, see:

TCH, "Due to a Hacker Attack, the Power of Half the Ivano-Frankivsk Region Was De-Energised".
UK, "National Cyber Security Strategy".
US, "Alert (Ir-Alert-H16-056-01), Cyber-Attack against Ukrainian Critical Infrastructure".
Case, "Analysis of the Cyber-Attack on the Ukrainian Power Grid".

attack on a drinking water treatment plant by unknown hostile actors in Florida, US, in January 2021 proves that this is not the case.

In this example, a US Cybersecurity and Infrastructure Security Agency (CISA) report in February 2021 confirmed that the attack had exploited basic cyber vulnerabilities. In doing so, the attacker changed the settings on one of the plants systems to increase the amount of a caustic chemical called sodium hydroxide being put into the water to a dangerous level. Though plant personnel noticed the change and acted before contaminated water could enter the local drinking supply, the event could have led to a massive human impact.

When examined in detail, CISA noted that the plant was using the outdated Windows 7 Operating System (OS) which, as it is no longer supported by Microsoft, could be expected to have unpatched security vulnerabilities. Furthermore, the plant also had systems connected directly to the public internet with no form of perimeter protection such as firewalls. Finally, workers in the plant were employing a single password across multiple systems and users. Collectively, these basic and avoidable vulnerabilities allowed easy access for the hostile actor. With the result being that a real layer system came close to a significant human impact across the Florida region, it shows that the lessons of the Ukrainian and other cyber attacks have not been universally learnt[550].

Though it is acknowledged that neither the Ukraine nor Florida examples are air power related, it is not hard to imagine a scenario in which both could have significantly disrupted the delivery of air power. For example, air bases rely on power for the functioning of airfield lighting, through to air traffic control, maintenance and beyond. Though most military airfields will have local backup generators, these are not a long-term solution and are unlikely to provide all the power requirements. Therefore, if vulnerabilities in the electrical supply of an air base were to be targeted in the same manner as was achieved in Ukraine, all

[550] For the CISA report, see:
US, "Alert (Aa21-042a) – Compromise of Us Water Treatment Facility", ed. Cybersecurity & Infrastructure Security Agency (CISA) (2021).
For analysis of the water treatment plant attack, see:
J. MacColl and S. Dawda, "Us Water Plant Suffers Cyber-Attack through the Front Door", *RUSI Commentary,* (2021).

power could be lost, and long-term operations put at risk. In such a scenario, air power is denied as effectively as a kinetic strike on the runway.

Alternatively, in terms of the water plant, air power is, as discussed above, reliant on people for its delivery and operation. If the drinking water supply to an air base was targeted and the personnel on it poisoned, operational effectiveness would drop immediately. Given these examples, the importance to air power of preventing cyber vulnerabilities in real layer critical infrastructures not only on its air bases but also in its supporting elements becomes evident.

Supervisory Control and Data Acquisition (SCADA) Systems

Delving into this issue further, a niche but important example of infrastructure vulnerabilities that could disrupt aviation are SCADA systems[551]. Developed to automate and optimise industrial processes, SCADA systems now form the core of virtually all industries. Integral to everything from transport to power it was, for example, attacks on the SCADA systems of both the Ukrainian power grid and Florida water plant that caused the impacts discussed above[552].

Despite their universal importance, a troubling reality has emerged in which most SCADA systems were never built with security in mind. Previously employed on industrial networks in remote locations or enclosed production lines, it had routinely been assumed that as the systems were air gapped from both other networks and the internet[553], or were interconnected via dedicated point-to-point links[554], it would be impossible for an external attack to occur.

[551] SCADA systems are also sometimes referred to as Industrial Control Systems (ICS). However, the term ICS is more clearly defined as an umbrella term for both SCADA and Distributed Controls Systems (DCS). The later, DCS, is a type of process control system that connects controllers, sensors, and terminals rather than the physical processes controlled by SCADA systems. For a simple overview of the definitional distinctions, see:
Securicon, "What's the Difference between Ot, Ics, Scada and Dcs", (2019).

[552] For further depth on Governmental and academic analysis of the cyber vulnerabilities in SCADA systems, see:
UK, "The Uk Cyber Security Strategy Protecting and Promoting the Uk in a Digital World".
A. Nicholson et al., "Scada Security in the Light of Cyber-Warfare", *Computers and Security,* 31, no. 4 (2012).
Case, "Analysis of the Cyber-Attack on the Ukrainian Power Grid".
N. Tariq, M. Asim, and F.A. Khan, "Securing Scada-Based Critical Infrastructure: Challenges and Open Issues", in *5th International Workshop on Cyber Security and Digital Investigation* (2019).

[553] Air-gapping involves the removal of all physical connections and wireless capabilities from every element of a network.
Wired-Staff-Writer, "Extreme Security Measures for the Extra Paranoid", *Wired*, 12 September 2019.

[554] Point to Point links, often referred to as P2P or P2P topologies, are a simple and secure network design which connects 2 elements of a network together using a dedicated physical link. Not limited to Local Areas Network (LAN) in a small

However, mirroring wider developments in the centralisation of control, SCADA systems have become increasingly networked. Now interconnected with other SCADA systems and usually a central control function, they routinely use the internet as a bearer for their communications. With security provision failing to keep pace in ensuring these connections are adequately protected, vulnerabilities within SCADA systems are being increasingly targeted by hostile actors[555].

Despite rising concerns in this area, many companies operating SCADA systems are not only failing to update security measures to manage vulnerabilities but are also failing to report cyber breaches and incidents. A situation made possible by most countries only requiring cyber incidents involving personal or financial information to be reported, statistics produced by Dell in 2015 identified a doubling of SCADA breaches. With Dell warning that these statistics were unlikely to show the totality of the problem, it signalled a troubling trend[556]. This assertion was reinforced by a 2019 industry report published by Fortinet which highlighted that 6 in 10 organisations operating SCADA systems had experienced a cyber breach in the preceding year[557]. Based on this, it would appear to be a trend that is set to continue.

In a similar vein to other real layer examples, SCADA vulnerabilities in military aviation have not been publicly reported. However, other examples indicate why the issue must be of concern. For example, media reporting in 2011 confirmed that vulnerabilities in the SCADA systems of pumps belonging to a US water company had been compromised[558]. Allowing attackers to turn the pumps on and

geographic location, P2P links can be used over long distances where either the confidentiality, integrity or availability of the information being processed requires a high degree of assurance. The limitation, however, is cost. A dedicated physical connection over a long distance requires significant engineering support.

S. Sohalianwar, "Point to Point Topology; Advantages and Disadvantages", *Computer Technology Topology,* (2019).

N.R. Rodofile, K. Radke, and E. Foo, "Extending the Cyber-Attack Landscape for Scada-Based Critical Infrastructure", *International Journal of Critical Infrastructure Protection,* 25 (2019).

[555] For discussions on SCADA systems and increasing concerns over associated cyber vulnerabilities, see:

V.M. Igure, S.A. Laughter, and R.D. Williams, "Security Issues in Scada Networks", *Computers and Security,* 25, no. 7 (2006).

B. Miller and D. Rowe, "A Survey of Scada and Critical Infrastructure Incidents", in *1st Annual conference on Research in Information Technology* (2012).

[556] Dell, "Dell Annual Threat Report ", (2015).

[557] Fortinet, "Independent Study Pinpoint Significant Scada/Ics Security Risks", (2019).

[558] F.Y. Rashid, "Cyber-Attackers Breach Scada Network, Destroy Pump at Water Utility'", *eweek*, 18 November 2011.

off repeatedly until they burnt out, it can be surmised that a similar attack focused on the fuel pumps of an air base could either disrupt or cease supplies.

Going further, this example can also be overlaid with the major disruption to civilian flights which occurred at Manchester Airport when the pumps in its' fuel infrastructure failed[559]. Combined with Russia displaying a credible intent in Estonia in 2007 to employ cyber effects against the infrastructure of its adversaries, one quickly builds a concerning picture[560]. Specifically, were SCADA systems on an air base to be targeted by a credible attacker, the result will be a major loss of critical infrastructure and, thereafter, a significant impact on air operations.

A Credible Concern

Though the above discussion only offers a small window into the real layer vulnerabilities that could challenge air power, the scope of the problem remains undeniably large. This assertion is illustrated by government agencies including the US DHS who have warned that Advanced Persistent Threats (APT) are actively targeting multiple sectors from the government through to aviation[561].

With these potential exploitations also having successfully exploited real layer vulnerabilities in other sectors, it is not without reason to expect similar incidents to occur in the confines of air power. Based on this, there is a strong argument that the real layer vulnerabilities represented in this discussion pose a credible concern to air power which, if not actively understood and managed, will result in adverse operational impact. If this were to occur, as highlighted in the other layers discussed above, the viability of air power might be questioned. From there, the ability of a state to rely on air power to survive and thrive in the international system may be lost.

[559] BBC, "Who, What, Why: How Can an Airport Run out of Fuel?", *BBC News Online*, 7 June 2012.
[560] Ottis, "Analysis of the 2007 Cyber-Attacks against Estonia from the Information Warfare Perspective".
[561] S. Sharwood, "Us Energy, Nuke and Aviation Sectors under Sustained Attack", *The Register,* (2017).

Conclusion

Building on the previous Chapter which argued that air power forms a pivotal capability in maintaining a state's role in the realist-constructivist sense, this discussion turned to consider cyber vulnerabilities. The first of two elements which, in combination, will be argued may cause the loss or compromise of air power, the discussion opened by challenging a common assumption that the sources of cyber vulnerabilities are limited to digital networks. Expanding the interpretation using the *Cyber Primer's* 'Layers of Cyberspace' model, an introductory section set the scene for an exploration of how cyber vulnerabilities across the people, information and real layers may impact on air power[562].

Turning first to the people layer, the discussion noted that even if digital information is 'the lifeblood of Defence', people remain a keystone to air power[563]. Acknowledging the scale of the task in examining people related vulnerabilities, the discussion chose to narrow the scope by distinguishing between 'outsiders' and 'insiders'.

Initially considering outsiders, a group intuitively understood as anyone external to an organisation, it was concluded that though important they represented a threat rather than a vulnerability. Having highlighted that the group would be considered within a subsequent exploration of the cyber threat to air power, the discussion turned to insiders.

A group defined as those with legitimate access to an organisation's sensitive material, the history and importance of the insider was considered before the discussion further subdivided the topic into non-malicious and malicious insiders. With both groups found to represent a concerning risk to air power, it was concluded that air forces must both recognise the issues people create and employ non-technical measures to actively manage the associated cyber vulnerabilities.

[562] UK, "Cyber Primer", 5.
[563] "Joint Service Publication (Jsp) 441 – Managing Information in Defence – Part 1: Directive", 1.

Moving onto the information layer, the discussion found an environment that is more readily identified by technologists as core to cyber. Defining the layer as representing the connections between network nodes and their logical constructs, it was explored how NextGen technologies had profoundly changed military aviation.

Acknowledging that 'timely, accurate and untampered' digital information was now essential to the projection of air power, it was noted that due to the scope and complexity of the issue it was again necessary to divide the topic[564]. First considering direct vulnerabilities, an area defined as weaknesses that could be directly exploited by hostile actors, the discussion used the examples of UADs and contractor systems to illustrate the breadth of the problem.

Next, examining indirect vulnerabilities, it was considered how the compromise of components in the supply chain may be both the hardest to identify and, ultimately, the most impactful vulnerability in the information layer. Employing counterfeit computer chips and malware on hard drives as illustrative examples, the question of whether concerns had been over exaggerated was finally examined. Though accepting that a 'Cyber Pearl Harbour' through an information layer vulnerability had not yet occurred, it was concluded that expecting the worst by approaching vulnerabilities with prudent concern was the only viable path to assuring the future of air power.

Finally considering the real layer, the Chapter drew comparisons with critical infrastructure to provide a lens through which to examine the topic. Noting how air operations are reliant on an air base's critical infrastructure, it was asserted that digital enablement has made the challenge of protecting infrastructure increasingly difficult.

With limited air power specific examples of real layer cyber vulnerabilities in the public domain, this assertion was illustrated using related examples. This

[564] De Cerchio, "Aircraft Systems Cyber Security", 2.

included the exploitation of vulnerabilities in the Ukrainian power grid in 2015 and SCADA systems. Noting that government agencies continue to highlight attempts to exploit such vulnerabilities, it was concluded that there is a strong argument for air forces to be concerned by the impact real layer exploitations could have on air operations.

Through its discussion, the Chapter articulated how on different levels cyber vulnerabilities can negatively impact air power. Not only justifying the element's inclusion in any examination of cyber risk, it added further evidence to the previous discussion on the 'first cause'. Specifically, with states increasingly reliant on air power to survive and thrive in the international system, they must procure and operate air platforms that can consistently meet the defence tasks required of them. If they fail to achieve this, states will be unable to maintain the role to which they aspire and may, in extremis, experience a threat to their survival as they are challenged by realist forces. Given this, when employing air power in this age of digital enablement, it becomes necessary to question whether the air platforms and supporting systems being operated are sufficiently robust.

In considering this question through the lens of the concepts that have been introduced, significant concerns over the viability of air power are raised. Derived through the plethora of existing and potential cyber vulnerabilities detailed across all three layers, one must conclude that contemporary forms of air power exhibit a real potential of compromise to a point of operational ineffectiveness. However, in balancing this, it must also be recognised that in isolation cyber vulnerabilities are not the sole cause of air power's cyber risk. Rather, it is only when combined with credible cyber threats that the potential cyber risk materialises.

Responding to this, the thesis will in Chapter 5 examine the cyber threats which contemporary air power is exposed to. Forming the last piece in the 'puzzle' of the 'three causes', this will complete the contention that cyber risk presents a credible challenge to air power. By doing so, it will set the scene for Part 3 of the thesis which through a series of case studies will test the assertions made in Part 2.

Chapter 6: The 'Third Cause' – Cyber Threats

Introduction

Offering the final element to Part 2 of the thesis, this Chapter will in the form of cyber threats explore whether hostile actors have the intent and capability to exploit the cyber vulnerabilities discussed above. If shown to be the case, this will prove that in combination the two elements have the capacity to undermine the viability of air power and endanger its' position as a keystone capability. In such circumstances, the concerns raised in the 'first cause' on state reliance of air power would be tested and states may lose the roles to which they aspire.

To begin this examination of cyber threats, the discussion will initially consider the evolution and diffusion of cyber power and influence. With digital information identified as a strategic resource, the manifestation of cyber threats will be explored. Achieved through a review of the relevance of cyber in state-on-state conflict, it will be deduced that cyber is not yet sufficiently advanced to undermine the relevance of air power.

Having accepted this initial conclusion, the potential future cyber threat to air power will explore how cyber might undermine air power through two distinct categories: the direct targeting of air platforms and indirect or left-of-launch attacks. Based on its findings, the Chapter will draw the discussion to a close by examining whether cyber threats are likely to undermine the strategic relevance of air power. Responding to this, it will be concluded that air power's continued pre-eminence in conflict will motivate states to develop cyber effects that counter the capabilities conventional dominance.

Finally reviewing the broader discussion, the concluding section will assert that by offering the final piece in the thesis' three causes the Chapter will demonstrate that the cyber risk to air power is not only possible but highly credible. Likely to prevent the strategic effectiveness of air power, there is a strong possibility that states may, if effective mitigations to the risk are not achieved, struggle to not only thrive but possibly even survive in the contemporary realist-constructivist environment.

Cyber Power and Influence

Evolution and Diffusion

To embark on this exploration of cyber threats to air power, it is necessary to understand how the concepts of cyber power and influence have emerged and become embedded in contemporary society. Considering the foundation to this, we must recognise mankind's ability to innovate that for millennia has driven technological progress. Though in many periods of history this has been slow, the world has in the last 400 years experienced three relatively short periods of remarkable advancement.

In the first, the Industrial Revolution of the 18th century, innovations from mechanised manufacturing to the steam engine impacted daily life. Allowing the UK as a key innovator to build a global Empire, it proved how innovation aligns to shifts in power and influence[565]. Occurring again in the late 19th and early 20th centuries, the Second Industrial Revolution initiated a period of standardisation and industrialisation. Dispersing control from not only colonial powers but also states themselves, the impact of innovation on power and influence was again demonstrated[566].

Though the technologies which ushered in these first two revolutions remain relevant, Jaincke and Jacob note that in the latter half of the 20th century a Third Industrial Revolution emerged[567]. Initially evident in the 1970s development of digital technologies, the growth of these would follow Moore's Law that

[565] Deane, *The First Industrial Revolution* 2.

[566] Haradhan, "The Second Industrial Revolution Has Brought Modern Social and Economic Developments", 5.

[567] M. Jaincke and K.H. Jacob, "A Third Industrial Revolution," in *Long-Term Governance for Social-Ecological Change* ed. K. Eisenack and K.H. Jacob (Abingdon: Routledge, 2013), 49.

processing power will on average double every two years[568]. Leading to digital technologies becoming entwined in every facet of modern life, the Third Industrial Revolution transformed the world into a post-industrial or information society[569].

Arguably having the most profound societal, political, and economic impact of all three revolutions, its far-reaching effects not only redistributed but redefined power and influence. Beyond this, a Fourth Industrial Revolution characterised by advances including AI and gene editing is further poised to 'blur the line between the physical, digital, and biological worlds'[570]. Given these expected advancements, it is logical to conclude that digitally-led societal upheavals will continue[571].

As part of these developments, a 'sea change' has been experienced in how information is not only collected, stored, processed, and communicated but harnessed to achieve influence[572]. Emerging as a strategic resource, digital information held and analysed in bulk is now as valuable and influential as capital or labour were in the industrial age[573].

Offering a new form of weaponisable power that can achieve influence at relatively low cost, these developments have disrupted and eroded traditional hierarchies. In Nye's view historically unique, such change has allowed conventionally weak states to achieve significant relative gains in power and influence[574]. Occurring alongside trends including globalism, the information

[568] Moore's Law predicts that every 2 years the industry would be able to fit twice as many transistors onto a chip. Whilst advances in technology have changed the components, Moore's Law has stayed consistent with digital processing power on average doubling every 2 years.
Moore, "Cramming More Components onto Integrated Circuits", 1.
L. Eckhout, "Is Moore's Law Slowing Down? What's Next?", *IEEE Computer Society*, no. July/August (2017): 4.

[569] It is noted that though this thesis focuses on the development of IT as the defining feature of the Third Industrial Revolution, other academics including Rifkin consider it to encompass not just digital technologies but the emergence of green technologies and the shift away from the highly polluting means of production employed in the First and Second Industrial Revolutions.
Lyon, "From 'Post-Industrialism' to 'Information Society: A New Social Transformation? ", 584.
Riftkin, "Leading the Way to the Third Industrial Revolution", 5.

[570] Schwab, *The Fourth Industrial Revolution* 99.

[571] For an overview of the factors leading to the Fourth Industrial Revolution, see:
UK, "Policy Paper: Regulation for the Fourth Industrial Revolution - Energy and Industrial Strategy", ed. Secretary of State for Business (2019).

[572] Arquilla and Ronfeldt, "Cyberwar Is Coming!", 143.

[573] Ibid.

[574] For a how digital information has redefined previous norms in power, see:
Nye, *Cyber Power*, 1.
Arquilla and Ronfeldt, "Cyberwar Is Coming!", 144.

society has created an era of digitally enabled multipolarity in which super and great states might hold more relative influence but will, nonetheless, find 'the stage more crowded and difficult to control' than before[575].

Defining Cyber Power and Influence

In recognising this post-industrial reality and charting how it creates the cyber threats which might target air power, it is necessary to define what form cyber power and influence have taken. Considering first cyber power, it is, as with the overarching concept of power, 'elusive and difficult to measure'[576]. Despite this, many have tried.

Approached from a positivist perspective, Willett describes cyber as a 'formidable instrument of national power'. Drawing parallels to air power, he argues that like identifying 'tier one' air power states through an assessment of capabilities, cyber power can be objectively quantified by examining resources[577]. An example of this is offered by the Belfer Centre's *National Cyber Power Index 2020.* Plotting quantitative evaluations across 7 indicators, the index assesses cyber power against intent and capability. In doing so, the Belfer Centre identifies the world's top 10 cyber states[578].

Alternatively, interpretivist approaches to define cyber power tether actors to a set of subjective indices. For example, Betz and Stevens argue that cyber power is best conceived as a 'family' of related dynamics[579]. In this, they contend that to understand the concept one must regard it as a variety of powers 'that circulate in cyberspace and which shape the experience of those who act in and through

[575] Nye, *Cyber Power*, 1.
R. Haass, "The Age of Nonpolarity", *Foreign Affairs,* (2008): 47.

[576] Nye, *Cyber Power*, 2.

[577] Willett, "Assessing Cyber Power", 87.

[578] The indicators used by the Belfer Centre are surveillance, defence, intelligence, information control, financial, commercial and norms. Each indicator is also sub-divided into 7 to 8 sub-categories.
Voo et al., "National Cyber Power Index 2020".
Other examples of quantitative ranking of cyber powers include:
ITU, "Global Cybersecurity Index, Version 4 ".
Hathaway, "Cyber Readiness Index 2.0: A Plan for Cyber Readiness".
Economist-Intelligence-Unit, "Cyber Power Index".

[579] Betz and Stevens, *Cyberspace and the States: Toward a Strategy for Cyber-Power*, 52.

them'[580]. Developing this premise, Kuehl concludes that cyber power is in isolation unimportant. Rather, it is not through positivist indices but the harnessing of power in cyberspace to achieve real-world strategic objectives that cyber finds its relevance[581].

Displaying synergies with Hart's overarching definition of power and influence[582], Kuehl expands on his position defining cyber power as 'the ability to use cyberspace to create advantages and influence events in other operational environments'[583]. In adopting Keuhl's definition, this thesis contends that cyber power, like all forms of power, is not absolute but relative. As such, cybers true value is only identified by understanding and qualifying the level of influence the use of cyber means can exert over resources, actors, or events external to the digital world.

Reflecting on this with reference to air power, it can be concluded that cyber has emerged as an undeniable source of power to be explored and harnessed by states. As with any source of power, however, it is a state's ability to harness its real-world influence that is pivotal. Therefore, the question for this thesis is whether cyber power has developed to a point at which states can deliver cyber threats that will meaningfully influence the real-world capability of air power. Before a clear assessment of this can be conducted, one must also appreciate the environments through which cyber power must be manifested if influence is to be achieved.

Operating Domains

To understand these environments, it is necessary to acknowledge the long lineage of discussion on where human conflict has evolved and, how within these realms, power is translated into threats that achieve influence. Within this, it is

[580] Ibid., 44.
[581] Kuehl, "From Cyberspace to Cyber Power: Defining the Problem," 41.
[582] Hart, "Three Approaches to the Measurement of Power in International Relations".
[583] Kuehl, "From Cyberspace to Cyber Power: Defining the Problem," 38.

noted that for academics and military professionals alike such environments are commonly referred to as domains.

Iteratively developed alongside advances in technology, these environmental domains began with land. Pivotal to all military endeavours which seek to exert control over 'a proportion of the earth' and influence the lives of those who live on it, the land domain is often viewed as core to state-on-state conflict[584]. Though retaining this position in the minds of many strategists, land was joined by maritime with the discovery of flotation and air with the advent of powered flight. Finally, by the late 20th century the fourth domain of space was added[585].

Though each of the four domains are unique, all share basic physical commonalities in that they interact and overlap. It has therefore been relatively straight forward for concepts designed for one to be applied to all. Taking international law as an example, the first to be regulated was land in 1864 through the Geneva Convention. Providing the basis for International Humanitarian Law (IHL) and the Law of Armed Conflict (LoAC), it regulated how the land domain was to be understood and used. Though meant to be unique, physical commonalities allowed its application with only limited domain specific amendments to maritime, air and space[586].

Whilst this regulation endures into the 21st century, the emergence of the information society added complexity. Though no commentators have suggested that cyber will replace the traditional domains, digitisation has permeated land, air, maritime and space making modern conflict 'as reliant on fast network

[584] For a summary of the land domain, its enduring importance, and the challenges it brings, see:
D.E. Johnson, "An Overview of Land Warfare", (The Heritage Foundation 2018).
T.R. Fehrenbach, *This Kind of War: The Classic Military History of the Korean War* (Dulles: Potomac Books, 2008), 290.

[585] Libicki, "Cyberspace Is Not a Warfighting Domain", 321.

[586] For relevant documents which combine to create the IHL, see:
H.S. Levie, "History of the Law of War on Land", (International Review of the Red Cross, 2000).
ICRC, "The Geneva Conventions of 1949 and Their Additional Protocols", (International Committee of the Red Cross, 2014).
UN, "Oceans and Law of the Sea. The United Nations Convention on the Law of the Sea".
ICAO, "Chicago Convention on International Civil Aviation", (International Civil Aviation Authority 1944).
UN, "2222 (Xxi) – Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space", (United Nations, 1966).

connections as [it is] on breathable air'[587]. In response, states and academics alike have attempted to define and understand the digital environment.

In examining these attempts, it is noted that despite the emergence of digital-means in the 1970s it was not until the early 2000s that meaningful academic thought would be applied. Notable in these early discussions was the 76th edition of the US Naval College's *Blue Book.* Published in 2002 it explored the nature of, and considerations surrounding, cyber operations[588]. Though the world's attention would be diverted by conventional terrorism in the wake of 9/11, cyber incidents in the late 2000s including the alleged Russian-sponsored attacks on Estonia and Georgia would reinvigorate attention[589].

Through this process states began to identify cyber as a high priority for national security[590]. A realisation that led NATO to collectively recognise cyber as a pressing threat in 2010, the organisation finally took a doctrinal lead in 2016 by identifying the concept as an operating domain in equal stature to the traditional four[591]. However, when reflected on, this declaration and the wave of state-centric cyber strategies that would follow remain conceptually problematic.

Exploring this Libicki comments that in labelling cyber as a domain the natural tendency is to apply traditional military attributes such as mass, speed, and fires.

[587] The quote is taken from the Armed Forces Journal's discussion on military reliance on digital networks and systems. This view was underlined by General Mattis, a former USMC General and US Defence Secretary, who commented in 2014 that US forces were no longer able to operate 'when [digital] systems go down'.
Staff-Writer, "Practice Disconnected".
Mattis, "Military High Tech Leads to Big Graft."

[588] The 'Blue Book' is a series of US Naval College publications dating back to 1901 which for over a century have pushed the boundaries of understanding on international law. This 76th edition represented the first meaningful attempt to examining what was at the time increasingly viewed as a potential 'cyber domain'.
Schmitt and O'Donnell, "Foreword – Computer Network Attack and International Law".

[589] For detail on the Estonia cyber attacks, see:
Ottis, "Analysis of the 2007 Cyber-Attacks against Estonia from the Information Warfare Perspective".
A. Ansip, "Estonian Pm Insists That Cyber Attacks Came from Kremlin Computers", *The Baltic Times*, , 6 August 2007.
For detail on the Georgia cyber attacks, see:
J. Markoff, "Before the Gunfire, Cyberattacks", *The New York Times*, 12 August 2008.
CNN, "2008 Georgia Russia Conflict – Fast Facts", *CNN Editorial Research*, 31 March 2020.

[590] Examples of states identification of cyber as a high priority include the following:
US, "National Security Strategy", ed. President of the United States (2010), 27.
UK, "A Strong Britain in an Age of Uncertainty: The National Security Strategy", ed. HM Government (2010), 11.
Russia, "Conceptual View Regarding the Activities of Armed Forces of the Russian Federation in Information Space ", (Russian Federation 2011).

[591] For NATO's 2010 recognition of cyber, see:
NATO, "Strategic Concept: For the Defence and Security of the Members of Nato", (2010), 11.
For NATO's formal 2016 recognition of the cyber domain, see:
"Nato Cyber Defence - Nato Fact Sheet", (2016).

However, with these concepts holding little utility in a virtual space, he concludes that any move to do so undermines the digital environment. Furthermore, if the digital environment is viewed through the same lens as the traditional domains, military thinkers will, he asserts, be drawn into shifting emphasis from advantageous digital operations to controlling the domain for its own sake. Linked in Libicki's view to a traditional military tendency to apply narrow thinking where clarity is lacking, he concludes that cyber is not, as NATO claims it to be, an operational domain but a malleable man-made environment[592].

Notwithstanding the strength of this argument, Libicki himself acknowledges that whatever label is placed on digital operations, there remains an imperative for states to 'organise, train, and equip forces' in the medium of the digital environment[593]. Because of this, he accepts, the term 'cyber domain' might be sub-standard but is, in practicality, necessary. Offering a 'middle ground' it is likely that such pragmatic reasoning has been the driving factor behind the broad acceptance of cyber as a domain.

Regardless of the reasons for its acceptance as a domain, once it was defined as such, moves to understand, and regulate cyber became necessary. Though some, including the US, argued that 'cyberspace did not require a reinvention of customary international law', others, including NATO, disagreed[594]. To resolve this, NATO commissioned the *Tallinn Manual.* Published in 2013 and updated in 2017, the Manual described as 'a digital Geneva Convention' sought to position cyber in a conceptual space that fits seamlessly alongside the traditional four domains[595].

Focusing on an examination of international law and how it governs 'cyber warfare', the Manual does not specifically define the cyber domain. However, what it delivers is a causal, but authoritative, link between the term's 'domain' and 'cyber'. Underpinned by its Rule Set, the Manual ultimately dismisses Libicki's

[592] Libicki, "Cyberspace Is Not a Warfighting Domain", 326.
[593] Ibid., 333.
[594] US, "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World", ed. President of the United States (2011), 8.
[595] T. Wheeler, "In Cyberwar, There Are No Rules: Why the World Desperately Needs Digital Geneva Conventions", *Foreign Policy,* (2018).

argument that the digital environment is not a 'domain'[596]. It achieves this by reinforcing the view that states should treat cyber operations in the same vein as those of land, maritime, air and space.

It can be concluded that, on balance, the weight of academic thought alongside official doctrine and policy points towards the adoption of cyber as a legitimate fifth domain. Therefore, in considering the cyber threat to air power, we must explore the topic with cyber recognised as a distinct domain that is fundamentally separated from air power. However, in equal measure, as the maritime environment overlaps in its littorals with land, and with air and space sitting physically above land and sea, cyber through its invasive nature must be considered to envelop all.

In examining the cyber threat to air power, we must therefore focus on the 'cyber littorals' or, in more accessible terminology, where cyber power reaches beyond the digital domain and creates influence in the physical world of the air domain[597]. Based on this, the Chapter will now consider how cyber power can be translated into cyber threats that might influence the air domain. Within this, it will be concluded whether in doing so sufficient influence can be generated to undermine the strategic relevance of air power.

State-on-State Conflict: The Cyber Threat

Through the exploration of cyber power, and the translation of that power into influence through cyber threats, this Chapter has confirmed cyber as a strategic asset and a legitimate domain of operations. Building on this, it will now be examined how these forces manifest themselves. Through this it will be concluded whether the threats that emerge could meaningfully undermine the strategic relevance of air power. To begin, however, it is first necessary to centre and legitimise the thesis' focus on state, rather than non-state, cyber threats.

[596] For example, Rule 20 states that 'cyber operations executed in the context of an armed conflict are subject to the LoAC'. Further, Rule 30 defines a cyber attack as any 'cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.

Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*

[597] The concept of cyber littorals is taken from Withers. For depth, see:

Withers, "What Is the Utility of the Fifth Domain?", 133.

The origins of this discussion can be found in the early post-Cold War period. For example, writing in 1989, Ray argued that state-on-state conflict would soon be considered a 'quaint and unthinkable' concept[598]. Rallying against the realist assertion that conflict is inevitable, Ray pre-empted concepts including democratic peace that would by the late 1990s dominate Western political thought[599]. Contending that democracies will never go to war with each other, such post-Cold War assertions concluded that since democracy was spreading across the world, state-on-state conflicts would soon be a thing of the past[600].

Though understandable given the optimism of the post-Cold War period, Ray himself acknowledged in 2002 that conflict between states persevered. Though Ray credits this to the fact that not all major powers had in the 1990s become democratic, when viewed through the realist-constructivist framework the truth arguably runs much deeper[601].

From a realist perspective, for example, state-on-state conflict is inevitable. A fundamental factor of man's egotistic nature, its inevitability is illustrated by Thucydides famous 'trap' theory. Within this he contended that when an emergent state threatens the position of an established state war between the two will always occur[602]. With such developments inevitable in the cycle of human interaction, it would come as no surprise to Thucydides that, as shown by current tensions between the US and the PRC, his predictions are reoccurring[603].

[598] J.L. Ray, "The Abolition of Slavery and the End of International War", *International Organisation,* 43 (1989): 405.

[599] For a summary of this position of classical realism, see:
S. Molloy, "Truth, Power, Theory: Hans Morgenthau's Formulation of Realism", *Democracy and Statecraft,* 15 (2008): 8.
W.E. Scheuerman, *Hans Morgenthau: Realism and Beyond* (Malden, MA: Polity, 2009), 11.

[600] This 'assumed fact' of democratic peace was most notably referred to by US President Clinton in his 1994 State of the Union Address and later described by Christopher, the US Secretary of State under Clinton, to be a key 'pillar' of policy.
W.J. Clinton, "The 1994 State of the Union Address", ed. Clinton Digital Library (1994).
C. Warren, "Statement before the Subcommittee on Commerce, Justice, State and Judiciary," in *The Clinton Record on Democracy Promotion*, ed. T. Carothers (Carnegie Endowment for International Peace, 1992), 11.

[601] J.L. Ray, "Does Interstate War Have a Future? ", *Conflict Management and Peace Science,* 19, no. 1 (2003): 54.

[602] This premise refers to 'The Thucydides Trap' in which Thucydides through observations of the Peloponnesian War between Sparta and Athens argued that the rise of any state will inevitably lead to conflict at the point at which it surpasses the power of another established state.
Rusten, *Thucydides*
E.W. Robinson, "What Thucydides Teaches Us About War, Politics and the Human Condition", *War on the Rocks*, 9 August 2017.

[603] Contemporary commentators have linked the theory of the 'Thucydides' Trap' to the potential of conflict between the established US and the rising PRC. For analysis, see:
Marcus, "Could an Ancient Greek Have Predicted the Us-China Conflict?".

Building on this, other realists have reinforced Thucydides arguments[604]. A prime example is the Clausewitzian concept of absolute war. In this the aggressor will always be drawn to use utmost force to disarm their enemy by employing all the powers available to them[605]. Extrapolating this out to the contemporary environment, we can conclude that in the realist tradition state-on-state conflict continues to exist. However, when it occurs both air power as the preeminent conventional capability of the 21st century, and cyber as the newest conduit for conflict, will inevitably be employed. Therefore, the question for this thesis is not whether either capability will be used in state-on-state conflict, but which capability will dominate.

Though the realist argument is the starkest, the other element of this thesis' framework, constructivism, supports the conclusion. Whilst the paradigm was built on a lineage of idealism which fundamentally rejected the inevitability of armed conflict, a contemporary interpretation accepts that in certain circumstances conflict is inevitable[606].

For example, in his summary of constructivism Wendt argues that states will act towards all objects, including other actors, based on the meanings that they have for them. With this making a state act differently towards an enemy than a friend, they will engage in armed conflict when they perceive that their role or status is threatened[607]. When this occurs, a constructivist may not agree with Clausewitzian absolute war, but would accept that a state will use all means available to preserve their role and status.

Given these underpinnings, and reflecting on the consistent provision of proof from the Gulf War in 1991 to the fighting between Armenia and Azerbaijan in 2020

Allison, "The Thucydides Trap: Are the Us and China Headed for War?".
Zhang, "The Perils of Hubris? A Tragic Reading of 'Thucydides Trap' and China-Us Relations".

[604] J. Lindell, "Clausewitz: War, Peace and Politics", *E-International,* (2009).

[605] Clausewitz, *On War*

[606] Idealism can be viewed as a reaction to the horrors of the First World War and the desire for a socially constructed harmonious world that would challenge the dominance of realism and the apparent inevitability of war. This overview of idealism is derived from:
Ashworth, "Where Are the Idealists in Interwar International Relations?".
Wilson, "Idealism in International Relations," 332.

[607] Wendt, "Anarchy Is What States Make of It: The Social Construct of Power Politics", 399.

that conflict between states continues, we can conclude that Ray's initial predictions were wrong[608]. Going further, we can also conclude that given the nature of mankind to use all means at their disposal to succeed in conflict, operations in both the air and cyber domains can be confidently predicted. Given this, what must be established for the purposes of this thesis is what form cyber might take in state-on-state conflict and whether, when achieved, the threats that emerge from it will materially undermine the strategic relevance of air power.

The Current Cyber Threat to Air Power

Building on the above foundational understanding, it will now be examined whether cyber means have reached a level at which they can cross the digital threshold and deliver real-world influence able to undermine the relevance of air power. To address this, it is logical to begin with the origins of this cyber focused debate before following its lineage through to the current cyber threat to air power.

Emerging in the 1990s', a prominent early example of this debate was Arquilla and Ronfeldt's 1993 article which offered their predictions of an impending 'cyberwar'[609]. The first academics to employ the term, the conversation they ignited would continue into the 21st century spilling into politics as technology caught up with the conceptual foundations. In 2010, for example, Clarke, a counter-terrorism advisor to Presidents Clinton and G.W. Bush, warned that cyberwar would not only occur but would usher in a period that made 9/11 seem insignificant[610]. Echoed in 2012 by Leon Panetta, US Defense Secretary, who warned of an impending 'cyber Pearl Harbor', a clear consensus that cyber threats were not only emerging but would dominate the future of state-on-state conflict was being built[611].

[608] In January 1991 a US led coalition engaged in state-on-state warfare to remove occupying Iraqi forces from Kuwait. Though numerous state-on-state wars have occurred in the interim, a recent example of this trend continuing is found in October 2020 with a brief but bloody conflict between Armenia and Azerbaijan.

Ray, "The Abolition of Slavery and the End of International War", 405.

A. Taylor, "Operation Desert Storm: 25 Years since the First Gulf War", *The Atlantic*, 14 January 2016.

BBC, "Armenia-Azerbaijan: Why Did Nagorno-Karabakh Spark a Conflict?", *BBC News Online*, 12 November 2020.

[609] Arquilla and Ronfeldt, "Cyberwar Is Coming!", 144.

[610] Clarke and Knake, *Cyber War*, 261.

[611] Panetta, "Panetta Warns of Dire Threat of Cyberattack on Us."

Despite these dire predictions, such early utterances failed to define what a cyberwar would look like and how it might compete with conventional capabilities such as air power. As an example, Arquilla and Ronfeldt envisioned cyberwar as taking one of two forms: a 'netwar' in which societal conflicts would be fought in a non-kinetic manner over digital media or a 'cyberwar' in which information advantage would decide conventional conflict[612]. Though they offered these broad conceptions, they did not go so far as to argue which would dominate.

When considered with hindsight, digital skirmishes have to date trodden a path between both 'netwar' and 'cyberwar'. Though retaining in this a Clausewitzian 'war-like' quality of forcing an opponent to comply with one's will, events have generally adopted an asymmetric nature[613]. A reality which has attracted numerous titles from hybrid-warfare to grey-zone, states have synchronised cyber threats with military, political and civilian elements so that political ends are achieved without the use of cyber for kinetic effect[614]. In doing so, lines between not only combatants and non-combatants but war and peace have been blurred[615].

Though increasingly prominent, this 'hybrid' style of state-on-state conflict is not new. An approach defined by Mansoor as 'conflict involving a combination of conventional and irregular forces', examples can be identified as early as 400-200 BC in the writings of Chinese philosopher Sun Tzu[616]. However, what is new is the fact that rather than being a tertiary means firmly secondary to the conventional use of force, in the 21st century the injection of cyber has made digitally led hybrid warfare increasingly central to state-on-state conflict.

This argument is supported by reflecting on the contemporary strategies of numerous states and international bodies ranging from NATO's Comprehensive

[612] Arquilla and Ronfeldt, "Cyberwar Is Coming!", 146.
[613] Clausewitz, *On War* 18.
[614] Cullen and Reichborn-Kjennerud, "Understanding Hybrid Warfare".
[615] A.A. Nofi, *Recent Trends in Thinking About Warfare* (Alexandria: CAN Corp, 2006).
[616] For Mansoor's quote, see:
Mansoor, "Hybrid War in History," 2.
For Tzu's writing on the concept of hybrid means to win conflict, see:
S. Tzu, *Art of War* trans. L. Giles (Leicester: Allandale Online, 400-200 BC), 9.

Approach to the UK's Multi-Domain Integration (MDI)[617]. However, one of the first to actively adopt this approach at a state level was Russia in its development and employment of the Gerasimov Doctrine[618].

Though the title of Gerasimov Doctrine can be challenged through the argument that the writings of a single Russian Officer cannot be claimed to represent an entire doctrinal approach, the processes General Gerasimov explored are, if not the genesis of contemporary Russia strategy, certainly reflective of it. Shifting modern strategic thinking towards a vision in which politics and war inhabit the same spectrum, adoption of the approaches his writings encouraged have seen Russia harness digital information as a core strategic tool in achieving political aims. A prominent example of this was the 2008 Russian action against Georgia[619].

Triggered by a territorial dispute over South Ossetia, open hostilities began on 7 August 2008 with the Georgian Army attacking South Ossetia's separatist forces and Russia responding militarily on 8 August 2008[620]. Despite these being the first overt exchanges, subsequent reports indicate that cyber attacks against Georgia had begun in early July 2002[621].

This represented, according to Rid, the first time an independent cyber attack had been synchronised with a conventional military operation. In its occurrence, it displayed the initial operational use of a digitally led Gerasimov Doctrine strategy[622]. However, as Rid further notes, the attacks which focused on denying online services and defacing websites had little operational impact[623]. Given this,

[617] For the NATO Comprehensive Approach, see:
J. K. and Starling McInnis, C. G. , "The Case for a Comprehensive Approach 2.0: How Nato Can Combat Chinese and Russian Polical Warfare", ed. Scrowcroft Centre for Strategy and Security (Washington D.C: Atlantic Council 2020).
For MDI, see:
DCDC, "Multi-Domain Integration ", ed. Ministry of Defence (2020).

[618] Named after a Russian Chief of the General Staff, General Valery Gerasimov, the Gerasimov Doctrine is detailed in:
Gerasimov, "The Value of Science Is in the Foresight".
For further analysis of the Gerasimov Doctrine, see:
M.K. McKey, "The Gerasimov Doctrine", *Politico*, October 2017.

[619] D.J. Smith, "Russian Cyber Capabilities, Policy and Practice", *Contemporary Conservative Thought,* Winter (2014).

[620] CNN, "2008 Georgia Russia Conflict – Fast Facts".

[621] For example, *The New York Times* reported in August 2008 that US software company Arbor Networks had identified cyber based attacks against Georgia originating from Russia in early July 2020.
Markoff, "Before the Gunfire, Cyberattacks".

[622] Rid, "Cyber War Will Not Take Place", 10.

[623] Ibid., 14.

though it was a firm example of digitally led state-on-state conflict, Rid characterises the cyber elements as 'part of a warlike situation…[but not] in isolation an act of war[624].

Though the Georgian example was relatively limited, and far from being sufficiently impactful to undermine the strategic relevance of air power, the seeds it sowed led Russia to solidify their view that the boundary between war and peace had become blurred. With nonviolent measures of warfare considered equally effective as conventional means, the digital tools introduced in Georgia had transitioned to become a central tool of Russian warfare[625].

This assessment is underlined by events in the Ukraine from 2014. Historically considered by Russia a border region of its greater territory rather than a political entity, tensions between the two have since the end of the Cold War been persistent[626]. A factor heightened in the Crimean Peninsula which continues to serve as the home port for the Russian Navy's Black Sea fleet, attempts to seize control of the area fitted neatly within President Putin's long-term aim of reasserting regional dominance[627].

When this seizure was enacted from February 2014 onwards, the world would witness Russian activity that was heavily influenced by the concepts of hybrid-warfare. Though the spearhead would be alleged local militia armed with Russian weapons, the Gerasimov Doctrine would also be evident in numerous other areas[628]. Of these, cyber was notable. Described by industry commentators as a 'digital blitzkrieg', a NATO cyber security spokesman commented that between

[624] Ibid., 10.

[625] This assessment is supported by General Gerasimov who wrote in 2013 that in his estimation the rules of warfare have now changed with conflicts modelled on the Arab Spring predictive of future wars where non-military actors and political, economic, and other non-military means would be employed through digital means.

Lilly and Chersvitch, "The Past, Present and Future of Russia's Cyber Strategy and Forces", 132.

Gerasimov, "The Value of Science Is in the Foresight".

[626] With Ukraine a key part of the Soviet Union, and with it retaining strong familial ties with Russia, many Russians considered its separation from Russia a mistake at the end of the Cold War which threatened (and ultimately led to the loss of) the superpower status of Russia.

J. Masters, "Ukraine: Conflict at the Crossroads of Europe and Russia", *Council on Foreign Relations,* (2020).

[627] D. Mdzinarishvill, "Why Putin Took Crimea: The Gambler in the Kremlin", *Foreign Affairs,* (2016).

[628] J. Simpson, "Russia's Crimea Plan Detailed, Secret and Successful", *BBC News Online*, 19 March 2014.

2014 and 2017 you could not 'find a space in Ukraine where there had not been a [cyber] attack'[629].

Though it is acknowledged that other states have also employed cyber means to target adversaries, and Russia's use of cyber means was not as evident in its 2022 invasion of Ukraine, Russia is still recognised as an early initiator of digitally enabled hybrid warfare[630]. Treading the line between Arquilla and Ronfeldt's 'netwar' and 'cyberwar', one can predict, based on the success of these early Russian operations, that other states are likely to pursue similar strategies[631]. Given this, it could be concluded that cyberwar is not only here but has, in replacing the supremacy of conventional warfare, undermined the contemporary strategic relevance of capabilities including air power.

Challenging this argument, however, one can highlight recent examples of where the cyber element of contemporary operations has had no noticeable effect on either the continuance of conventional warfare or the relevance of air power. For example, in the 2020 conflict between Azerbaijan and Armenia media reports confirmed that the Turkish Air Force's use of armed UAVs and manned fast jet aircraft to support their Azerbaijani allies was decisive. Destroying Armenian armour in the field, the actions proved that conventional conflict continues to rage between states, and, in this, air power retains a dominant role[632].

Furthermore, in this conflict which drew in not just Azerbaijan and Armenia but their larger allies of Turkey and Russia, there has been no indication that cyber means have been used to undermine air power's strategic relevance. Though it is accepted that such means may have been employed but not reported, the

[629] For the Digital Blitzkrieg quote, see:

A. Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar", *Wired*, 28 June 2017; K. Geers, interview by D. Templeton-Raston, 26 December 2019.or

[630] Examples of other states who are reported to have engaged in cyber activity in an offensive state-on-state manner were explored in detail by the Centre for Strategic and International Studies (CSIS) in 2020.

CSIS, "Significant Cyber Incidents since 2006", (Centre for Strategic and International Studies (CSIS), 2020).

For related analysis, see:

Q. E. Hodgson et al., *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace* (Santa Monica: RAND, 2019).

Gerasimov, "The Value of Science Is in the Foresight".

Russia, "Doctrine of Information Security of the Russian Federation", (Russian Federation, 2016).

[631] Arquilla and Ronfeldt, "Cyberwar Is Coming!", 144.

[632] A. Gatopoulos, "The Nagorono-Karaback Conflict Is Ushering in a New Age of Warfare", *Aljazera Online*, 11 October 2020.

conflict could have been an ideal opportunity for a digitally capable state to undermine the air power of Turkey via cyber means.

Finally, Russia's 2022 invasion of Ukraine further underlines the argument. Though open-source reporting has indicated that Russia used cyber means to target Ukraine, conventional capabilities including air power have eclipsed the digital domain. For example, amongst Russia's cyber activities, its disruption of the Viasat Inc's KA-SAT satellite has been credited as the most significant event[633]. However, even when it is accepted that the impact spread beyond Ukraine, the event is not assessed to have provided Russia meaningful military advantage[634]. With other cyber attacks launched with the intent of causing disruption to Ukraine systems thought to have been largely unsuccessful in a military sense, but with heavy armour, artillery and air power successfully taking Ukrainian territory, the primacy of conventional capabilities appears to be proven[635].

Given these factors, it is evident that in contemporary conflict digital means delivered through the cyber domain are a reality and have, in certain perspectives, challenged air power. However, taken collectively the situation offers insufficient evidence to suggest that cyber has developed to a level at which it presents a credible threat to the strategic relevance of air power. Furthermore, with states such as Russia continuing to tread the line between 'netwar' and 'cyberwar' in a 'sub-Article 5' manner, it can be further concluded that this cyber threat has not in the state-on-state context developed to a point at which warnings of a 'cyber Pearl Harbor' are likely to be realised[636].

Based on the above discussion, it is concluded that cyber means do not at this time pose a credible threat to the conventional relevance of air power. This

[633] For an overview of the Viasat satellite attack, see:
Viasat, 30 March 2022, https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/.
For an assessment of the attack's linkages to Russia, see:
UK, "Russia Behind Cyber-Attack with Europe-Wide Impact an Hour before Ukraine Invasion", ed. Gov.UK (2022).

[634] J. Lewis, "Cyber War and Ukraine", (Center for Strategic and International Studies, 2022).

[635] For an assessment of Russian use of cyber in the 2022 conflict with Ukraine, see:
M. Orenstien, "Russia's Use of Cyberattacks Lessons from the Second Ukraine War", *Foreign Policy Research Institute,* (2022).

[636] Panetta, "Panetta Warns of Dire Threat of Cyberattack on Us."

assertion includes cybers potential replacement of air power as a preeminent capability in contemporary state-on-state conflict, and its ability to undermine air power's delivery of strategic effect.

The Potential Cyber Threat to Air Power

Though the above conclusion draws a clear line under whether the strategic value of air power is currently being threatened by cyber, history teaches that nothing is static. Within this, we must accept that whilst there are limited examples of cyber currently threatening air power in state-on-state conflict, it does not mean that the capability and intent to do so does not already or will not soon exist. To address this and answer the question of whether cyber could in the future undermine air power in state-on-state conflict, it is informative to look at wider scenarios.

Direct Cyber Threats

The first such wider scenario to consider is the potential redevelopment of direct cyber threats employed to significant effect in other areas. Through an examination of these, we can assess whether if rerolled to target air platforms they could impact the strategic relevance of air power.

Direct Targeting of Sensors to Deny Air Operations

An illustrative example to open this discussion is Operation Orchard. Commencing in the early hours of 6 September 2007, the operation witnessed Israeli Air Force (IAF) fast jets violating a ceasefire established in 1974 by entering Syrian airspace. Their target, the suspected secret nuclear weapons facility of al Kibar in the Deir ez-Zor desert, had been reportedly identified by US and Israeli intelligence as being weeks away from becoming operationally active.

Once this occurred, it was assessed, al Kibar would be able to produce weapons-grade plutonium[637].

In response, Israel decided that it was imperative to destroy the site. Achieved by the IAF in Operation Orchard, 'before' and 'after' reconnaissance pictures show the destruction of a rectangular building alleged to be the nuclear weapons facility. Subsequently, both the alleged use and its destruction have been confirmed by the International Atomic Energy Agency (IAEA)[638].

Despite these widely reported facts taken from a combination of media reporting and official Syrian statements, Israel has consistently denied that the IAF attacked al-Kibar. Rather, the Israeli authorities have maintained the line that the incident never occurred[639]. Given the fact that Israel routinely confirms their involvement in successful attacks, a principle which is key to their deterrence strategy, it is notable that in this circumstance they have chosen to deny involvement[640]. The reason for this, one might conclude, is that there are unique elements to the operation which both Israel and their US allies did not want to be publicly disclosed.

In exploring this, subsequent media analysis strongly suggested that this unique element is likely to be two cyber attacks which, in combination, are alleged to have made the strike possible. The first is reported to have taken place a year before the air strike. Using the Israeli intelligence agency, Mossad, it is believed that trojan horse malware was placed on the laptop of a Syrian official whilst he

[637] Horschig, "Cyber-Weapons in Nuclear Counter-Proliferation", 358.

[638] For background on the assessed requirement for and execution of Operation Orchard by the IAF see:

Kapan, "Air Power's Visual Legacy: Operation Orchard and Aerial Reconnaissance Imagery as Resus De Geurre", 61.

Horschig, "Cyber-Weapons in Nuclear Counter-Proliferation", 358.

For a summary of the IAEA's findings, see:

IAEA, "Implementation of the Npt Safeguard Agreement in the Syrian Arab Republic", (International Atomic Energy Agency 2011).

[639] For analysis of Operation Orchard including the Israeli denials, see:

V.E. Foolath and H. Stark, "How Israel Destroyed Syria's Al Kibar Nuclear Reactor", *Das Spiegel International*, 2 November 2009.

BBC, "Syria Fires on Israeli Warplanes", *BBC News Channel*, 6 September 2007.

[640] Numerous examples of Israeli strikes against its adversaries and their acknowledgement of these can be cited. One example involving Syria was on 20 July 2020 when the IAF stuck military sites controlled by Iran's Islamic Revolutionary Guard Corps. For depth, see:

J.A. Gross and T. Staff, "Idf Launches Airstrikes against Iranian Quds Force in Syria", *The Times of Israel*, 14 November 2020.

was staying in London[641]. Allowing files to be siphoned from the laptop, it is believed that the Israeli's obtained detailed plans for the al Kabir complex allowing them to prove its use and plan the attack.

Though an interesting example of cyber threats in the context of state-on-state conflict, this can be viewed as a routine example of digital espionage. Therefore, though such means could plausibly be used against air power, it does not provide an example of where cyber threats could directly undermine the viability of air power[642].

However, the next cyber phase to Operation Orchard is far more relevant. The key question which led commentators to consider this second element is, given the aging but still effective nature of Syrian air defences in 2007, how did the IAF manage to operate unscathed in Syrian airspace and destroy a valuable military target?[643] The answer, it has been suggested, is that the conventional strike was facilitated by a combination of 'electronic attack and cyber based network penetration' which allowed the blocking of Syrian air defences[644].

Examining the operation in more depth, media reports also suggest that these cyber attacks would have had to ensure that the Syrian air defence radar system went 'off the air' for the entirety of the strike[645]. Explored by industry expert Fulghum, the means to achieve this were likely provided by the US. Specifically, a version of the US developed 'Suter' airborne network attack system developed by BAE Systems and tested by US air platforms in Afghanistan was the most likely cyber delivery system[646]. Though remaining classified and not publicly

[641] A Trojan horse, or Trojan, is a form of malware that appears legitimate but can take control of a computer. It is designed to 'damage, disrupt, steal, or in general inflict some other harmful action on your data or network'.
Norton, "Malware – What Is a Trojan? ".

[642] For further detail on this initial cyber element to Operation Orchard, see:
K Zetter, "Mossad Hacked Syrian Official's Computer before Bombing Mysterious Facility", *Wired*, 11 March 2009.
Foolath and Stark, "How Israel Destroyed Syria's Al Kibar Nuclear Reactor".

[643] Though it is acknowledged that in 2007 Syria was believed to be operating an air defence system based on Russian technology developed in the 1970s, it was still assessed to have up to 150 Surface to Air Missile (SAM) batteries providing active overlapping coverage of the country. Given this, the threat to IAF aircraft attempting to strike al Kabir would have been significant.
A.H. Cordesman, "Syria's Uncertain Air Defence Capabilities", *Centre for Strategic and International Studies*, no. 6 May (2013).

[644] Horschig, "Cyber-Weapons in Nuclear Counter-Proliferation", 358.

[645] L. Page, "Israeli Sky-Hack Switched Off Syrian Radars Countrywide'", *The Register*, 22 November 2007.

[646] D. Fulghum, "Areas Blog (April 2007)", *Aviation Weekly*, April 2007.

discussed by either the US or BAE Systems, this technology which can be carried on airborne platforms locates enemy emitters before directing data streams into them. Allowing the user 'to invade communications networks, see what enemy sensors see and even take over as systems administrator', it provides an attacker the ability to manipulate defensive systems so that approaching aircraft cannot be seen[647].

Assuming that 'Suter' or a similar capability was used in Syria by the IAF, it represents a significant cyber development within the long-standing suite of means in the Suppression of Enemy Air Defences (SEAD). Stepping away from a previous reliance on Electronic Counter Measures (ECM) to 'jam' radar signals, its effective use would act to protect aircraft against 'increasingly high-tech anti-air defenses'[648]. In equal measure, however, if this technology is as effective as it appears to be in a SEAD role, then it is equally plausible that similar cyber means could be rerolled to undermine the strategic effectiveness of air power.

Though an interesting proposition, the question is whether this use is 'science fiction' or 'science fact'. Though public discussions in this area are limited, some studies have argued that the targeting of air platforms using similar cyber means is both possible and becoming more likely. When taken in the context of broader writings on similar cyber techniques illustrated through other scenarios, the evidence for 'science fact' becomes compelling.

Exploring one such example, Strohmeier et al identify the increasing viability of states directly targeting an adversary's air power via their wireless communications networks[649]. Focusing on the proliferation of Software-Defined Radios (SDR) which have largely replaced their hardware-based predecessors in airborne communication[650], they argue that insecurities in the proprietary

[647] W. Carrol, "A Closer Look at Israel's Syria Raid", *Defense Technology,* (2017).

[648] Quinian, "Jam. Bomb. Hack? New Us Cyber Capabilities and the Suppression of Enemy Air Defences".

[649] M. Strohmeier et al., "Assessing the Impact of Aviation Security on Cyber Power", in *8th International Conference on Cyber Conflict* (NATO CCDCOE 2016).

[650] SDR is a radio communication system which replaced the traditional use of hardware with software for the purposes of modulation and demodulation of radio signals. For further depth on SDR including the technologies use in aviation, see:

Garg, "Fourth Generation Systems and New Wireless Technologies," 233.

C. Adams, "Sdr Takes Flight", *Aviation Today,* (2013).

software even on military aircraft could allow a hostile actor to 'manipulate virtually all aspects of the wireless channels used by aviation protocols'[651]. If directed effectively, a hostile state could, as the technology in Operation Orchard is believed to have done, invade and manipulate an air platform's communications network undermining the viability of continued operations.

Examining the potential of such a threat materialising in state-on-state conflict, further analysis has suggested that SDR vulnerabilities could be accessed not only locally through physical access but also at distance through Radio Frequency (RF) interfaces. Once achieved malware could be introduced allowing an attacker to modify or prevent transmissions from devices which, in turn, could disrupt operations or, in extremis, allow an attacker to turn off devices[652]. Though such extreme examples have only been evidenced against commercial Internet of Things (IoT) devices rather than more complex military air platforms, the principles remain the same. Specifically, using RF means a state could directly target the communications systems of an adversary's air platform whilst airborne and prevent it from continuing to operate within a designated region.

Developed further with PRC activity in the South and East China Seas as an example, we begin to build a concerning picture of how air power could be significantly undermined in state-on-state conflict. Notably, if the PRC could harness such technologies to target air platforms they could 'blind' aircraft sensors and prevent their adversaries from effectively operating air power in the region[653].

[651] Strohmeier et al., "Assessing the Impact of Aviation Security on Cyber Power", 225.

[652] For an overview of this type of SDR vulnerability, see:

I. Ilascu to Bitefender Box December 2017, https://www.bitdefender.com/box/blog/iot-news/airborne-threat-software-defined-radio-attacks/.

For in-depth analysis including differing cyber threat-vectors, see:

Da Silva, Moura, and Galdino, "Classes of Attacks for Tactical Software Defined Radio".

[653] For overviews of the tensions between the PRC's expansionist tendencies and the US security alliance loosely associated under the grouping of the Free and Open Info-Pacific (FOIP), see:

US, "Us-China Strategic Competition in South and East China Seas: Background and Issues for Congress", ed. Congressional Research Service (US Congress, 2020).

"Territorial Disputes in the South China Sea - Global Conflict Tracker", ed. Council of Foreign Relations (2020).

Acting as a cyber enabled Area Access / Area Denial (A2AD) capability, this would undermine the long-standing use of air power to maintain oversight of, and counter, PRC expansionism. Allowing activities including island building, the construction of military bases and PRC claims of wide-ranging aerial and maritime sovereignty to go unchecked, there would be an increased likelihood that the PRC would move more aggressively towards regional hegemony[654].

Considered from the perspective of the PRC's US led adversaries, these cyber based tactics would likely remain below any traditional threshold for a conventional military response. Because of this, the might of the US, including its conventional land and carrier borne air power held in the region, would be politically limited in how it could be used in response to the expansionism. Ultimately, this would lead to the PRC's achievement of political aims across the South and East China Seas. Extrapolating this out to use by other states, it becomes evident that the direct employment of cyber means to target air platforms in flight could emerge as a credible threat to the strategic relevance of air power.

Direct Targeting of Unmanned Aerial Vehicles (UAV)

A second potential example of direct cyber attacks against air platforms is found within the digital fragility of UAVs. Discussed by Hartmann and Giles, they suggest that though cyber attacks on these air platforms are not prominently recognised, they are certainly not new[655]. Examined by Ly and Ly, four principal forms of cyber attack that UAVs are particularly prone to have been identified[656].

[654] Examples of the importance of air power and air supremacy within the South China Sea region to both the US and its allies and the PRC continue to be offered. For examples including Freedom of Navigation (FoN) activities, see:

Z. Williams, "China's Tightening Grasp in the South China Sea: A First Hand Look", *The Diplomat*, 10 June 2020.

S. Roblin, "Us Aircraft Carriers in South China Sea Make Needed Show of Force against Beijing", *NBC News*, 8 July 2020.

Staff-Writer, "China Protests Us Spy Plane Watching Drills", *Reuters*, 25 August 2020.

[655] Hartmann and Giles, "Uav Exploitation: A New Domain for Cyber Power".

[656] Ly, "Cybersecurity in Unmanned Aerial Vehicles (Uavs)".

The first two of these, password theft and Man in the Middle (MITM) attacks, are common cyber security concerns that do not pertain directly to this discussion. However, in the third Ly and Ly identify the potential disruptive effect of a Denial of Service (DoS)[657]. Requiring an attacker to flood a UAVs wireless connection with requests or packets, DoS attacks can inhibit communications with the UAV preventing its effective operation even when its external links are encrypted. If employed in state-on-state conflict, this could prevent UAVs from operating effectively in regions controlled by a technologically advanced adversary[658].

In their fourth example, GPS Jamming and Spoofing, Ly and Ly highlight that by either preventing a UAV receiving a GPS signal or replacing that signal with another feed an attacker could undermine effective operations or even gain control of the UAV. In the latter scenario, an attack would send false messages that modify the UAVs direction rather than produce distracting signals.

Though one might hope that military UAVs were protected from such attacks, the loss of a US Sentinel UAV and its capture by Iran in 2011 show that this is not the case. An event confirmed by US President Obama, it has been assessed that a vulnerability within the Sentinel's sensor system which controlled navigation was exploited by Iran[659]. Allowing the UAV to be redirected and landed on an Iranian airfield, the events proved how in state-on-state conflict UAVs can be simply 'stolen' making their operation in specific regions impossible[660].

[657] A DoS attack is conducted when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.
US, "Understanding Denial-of-Service Attacks', Security Tips".

[658] For a summary of potential DoS attacks on UAVs, see:
Ly, "Cybersecurity in Unmanned Aerial Vehicles (Uavs)", 5.
For a technical analysis of how such attacks are possible, see:
R.S. Miani et al., "The Impact of Dos Attacks on the A.R.Drone 2.0", in *XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR)* (Brazil2016).

[659] In a joint press conference with Prime Minister al-Maliki of Iraq on 12 December 2011 President Obama stated when asked about the loss of a US Sentinel UAV in Iran that 'I'm not going to comment on intelligence matters that are classified…[but] we have asked for it back. We'll see how the Iranians respond'. These comments built on media speculation and responded to Iranian claims that they have successfully brought down a US UAV.
B. Obama, "Remarks by President Obama and Prime Minister Al-Maliki of Iraq in a Joint Press Conference", ed. Office of the Press Secretary (The White House, 2011).
CNN, "Obama Says Us Has Asked Iran to Return Drone Aircraft", *CNN World*, 12 December 2011.

[660] For a summary of potential GPS attacks on UAVs, see:
Ly, "Cybersecurity in Unmanned Aerial Vehicles (Uavs)", 5.
For a summary of the Iranian example of using the cyber attack against a UAV, see:
Hartmann and Steup, "The Vulnerability of Uavs to Cyber-Attacks; an Approach to the Risk Assessment".
For depth on GPS spoofing against UAVs in general, see:
Humphrey, "Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil Gps Spoofing".

With the US Government alone allocating $3.7 billion in new spending on UAVs in the 2020 defence budget, it is evident that the use of these air platforms will continue to rise[661]. When aligned to the continued reporting of potential cyber attacks which can be launched against them, it can be argued that in state-on-state conflict the level of trust which should be placed in UAVs to deliver effect may be diminishing.

Returning to the PRC example to illustrate this, reports have indicated an increased US reliance on UAVs in the South China Seas to achieve political aims. For example, in 2019 the US was reported to have sold 34 UAV surveillance drones to its regional allies to increase oversight of PRC activity[662]. This was followed in September 2020 by reports that the US had deployed its own Reaper UAVs to the region[663]. Able to conduct both reconnaissance and kinetic strikes, this Reaper deployment significantly increased the US's regional capacity with the intent of curtailing PRC expansionism. However, if the PRC were able to harness the cyber means employed by Iran to target US UAVs it would again achieve a means of controlling the air and allow its expansionism to continue without the risk of conventional escalation. By doing so, the PRC would undermine the strategic viability of US air power.

Taken collectively, the above examples suggest that existing cyber threats to air power could, if re-purposed and directed appropriately, undermine the capability's strategic effectiveness. With the South China Sea used as an example, one might go so far as to argue that the PRC, or any other technically capable state such as Russia could, by capitalising on these cyber threats, achieve an unrivalled form of A2AD.

The Viability of Direct Cyber Threats

[661] J. Harper, "Spending on Drones Projected to Soar", *National Defence*, 15 March 2019.
[662] M. Stone, "Us to Sell 34 Surveillance Drones to Allies in the South China Sea Region", *Reuters*, 3 June 2019.
[663] EurAsianDesk, "From Ladakh to South China Seas, Us Deploys Its 'Most Lethal' Armed Drone to Check Chinese Machoism", *Eurasian Times*, 30 September 2020.

If the above discussion of direct targeting of air platforms using cyber means were truly 'science fact' rather than 'science fiction' one might ask why they have not already featured more heavily in state-on-state conflict? The response to this, and the reason why such measures may not be viewed as likely to undermine the strategic relevance of air power, is founded in the potential limitations of cyber attacks.

A central element of this is the concept of 'zero-day' exploits. Referring to a vulnerability that only becomes known to a system operator on the day it is used to conduct an attack, 'zero-day' exploits are considered highly effective. This is because unlike known vulnerabilities which an operator would have mitigated as far as practicable, 'zero-day' exploits are unguarded allowing an attacker to achieve their intent unhampered. In equal measure, however, they are hard to identify and usually only effective once. This is because as soon as they are used developers and operators will quickly produce security patches or deliver system redesigns to prevent further use[664].

Placing this in the context of air power and state-on-state conflict, a situation is presented in which a state could, through in-depth investigation, identify a 'zero-day' exploit on the air platform of an adversary. In response, it could use the exploit to disrupt air operations but, logic suggests, this could only be achieved once. Therefore, the attacker would not want to do so unless the strategic gain was significant. Furthermore, such an attack would not be effective for prolonged periods making the above A2AD example arguably implausible. Given these factors, it could be concluded that other than a single event such as Operation Orchard where the strategic gain is judged significant enough to use an exploit, the direct cyber threat to air power is limited.

Though this logic is convincing, Hartmann and Giles offer a counterbalance highlighting those cyber attacks against air platforms, or associated capabilities such as Syrian air defences, have routinely exploited significant and long-term

[664] For depth on zero-day exploits, see:
K. Hausken and J. W. Welburn, "Attack and Defense Strategies in Cyber War Involving Production and Stockpiling of Zero-Day Cyber Exploits", *Information System Frontiers,* (2020).

flaws in security measures. If appropriate measures had been implemented, they contend, most cyber attacks would have been impossible making air power impervious to cyber risks[665]. However, with examples such as UAV vulnerabilities being known about for a long time but still not effectively managed, it is likely that in most circumstances it will not be ‘zero-day’ exploits but long-term vulnerabilities that allow cyber means to undermine air power.

Given this factor, it can be concluded that as with many forms of conventional and non-conventional attack the potential of success depends not solely on the ability of the attacker but the ill-preparedness of the defender. If in the case of cyber the defenders have been lax in preparing for attack, the viability of cyber means to undermine the strategic effectiveness of air power is greatly enhanced. To address this question for air power, and therefore whether direct cyber threats to air platforms is credible, the thesis must in the next chapters explore how prepared states are and whether such preparedness varies between states.

Left-of-Launch Cyber Threats

The above discussion has shown how direct cyber attacks on air platforms could, if used effectively against an ill-prepared adversary, undermine the strategic viability of air power. Looking beyond this, it is also informative to consider how by learning lessons from other areas of operations states might use less direct but equally effective cyber means of targeting air power. Such a scenario can be found in the left-of-launch concept.

Originating in missile defence, left-of-launch grew from the US's response to the 1991 Gulf War[666]. Acknowledging that existing defences had failed to prevent Iraqi missile attacks on Israel, efforts to develop means to not only protect military forces but also civilian targets began[667]. Building on this, the imperative would later grow in line with the West's fear that ‘rogue nations’ including North Korea

[665] Hartmann and Giles, "Uav Exploitation: A New Domain for Cyber Power", 207.

[666] On 18 January 1991 2 Iraqi scud missiles were fired at the Israeli cities of Tel Aviv and Haifa. The intent was to draw Israel into the conflict and undermine Arab support for the US led Coalition.

BBC, "1991: Iraqi Scud Missiles Hit Israel - on This Day: 18 January 1991", *BBC News Online*, 18 January 2020.

[667] H.C. Kemp, "Left of Launch: Countering Theatre Ballistic Missiles", (Atlantic Council 2017).

and Iran were close to fielding missile technologies able to threaten targets as far afield as the US mainland[668].

The largely US led response was to develop a 'full spectrum' missile defence programme that would augment conventional, or right-of-launch, interception capabilities[669]. Leading to an aspiration for 'integrated, layered ballistic missile defence architecture' that would offer multiple opportunities to destroy missiles, the main left-of-launch thrust focused on non-kinetic means intended to prevent missiles from launching[670].

With this left-of-launch programme articulated in a 2014 memo to the Secretary of Defence, the US for the first time publicly acknowledged both its intent and cyber focus[671]. However, media reports indicate that the US had successfully used left-of-launch cyber means as early as 2012 to target North Korean missile tests[672]. Believed to have then been increased under President Obama, the aim of 'sabotaging test launches in their opening seconds' via cyber means became the core of the US left-of-launch strategy[673].

Reflecting on the alleged success of cyber based left-of-launch attacks and accepting that both academic and official discussions are focused entirely on missile defence, there is an argument that the concept is transposable to air power. Specifically, as the 2014 memo outlines, with the concept seeking to

[668] The concept of 'Rogue States' or the 'axis of evil' was infamously depicted as consisting of Iran, Iraq and North Korea by President G. W. Bush in his 2002 State of the Union Address. This characterisation built on previous rhetoric on the topic of potential US adversaries. For depth and analysis, see:

G.W. Bush, "The President's State of the Union Address", ed. The White House Archives (2002).

A. Lake, "Confronting Backlash States", *Foreign Affairs,* 73, no. 2 (1994): 45.

A. Homolar, "Rebels without a Consciences: The Evolution of the Rogue States Narrative in Us Security Policy", *European Journal of International Relations,* 17, no. 4 (2010): 718.

[669] For a discussion of the 'full spectrum' approach to missile defence, see:

A. Futter, "The Dangers of Using Cyber Attacks to Counter Nuclear Threats", *Arms Control Today,* 46, no. 6 (2016).

For an overview of the Patriot Advanced Capability 3 (PAC-3) as an example of 'right-of-launch' means, see:

Staff-Writer, "Patriot Missile Long-Range Air-Defence System", *Army Technology,* (2020).

[670] US, "Missile Defence Review (2019)", ed. Department of Defence (2019), IX.

[671] The 2014 memo was written by US Army Chief of Staff General Odierno and the US Chief of Naval Operations Admiral Greener. It was directed to the Secretary of Defence. For the memo, see:

J.W. Greenert and R.T. Odierno, "Memorandum for the Secretary of Defense: Adjusting the Ballistic Missile Defense Strategy", ed. US Department of Defense (2014).

For analysis of the memo, see:

R. Ellison, "Left of Launch", *Missile Defence Advisory Alliance*, no. 16 March (2015).

[672] In this example of the US targeting North Korean missile tests, media reporting suggests that the cyber attacks caused 'a large number of the North's military rockets to explode, veer off course, disintegrate in mid-air and plunge into the sea'.

P. Lewis and B. Unal, "Cyberattacks on Missile Systems", *Chatham House,* (2019).

[673] D.E. Sanger and W.J. Broad, "Trump Inherits a Secret Cyberwar against North Korean Missiles", *The New York Times*, 4 March 2017.

prevent missiles from launching it is logical to assert that the same left-of-launch concept via cyber means could be applied to air power to prevent air platforms from flying[674]. If achieved, the value of air focused left-of-launch cyber attacks on undermining the strategic relevance of air power within state-on-state conflict would be momentous.

To examine the viability of this application to air power it is instructive to reflect on the main avenues through which, in Lewis and Unal's assessment, cyber can be used to achieve left-of-launch missile defence[675]. In doing so, assertions on the likelihood of states applying these means to air power can be drawn.

Supply Chain

The first of Lewis and Unal's left-of-launch cyber means is targeting of the supply chain**.** Believed to be the means through which the 2012 North Korean missile launches were sabotaged, the foundations of a supply chain cyber attack involve the altering of software or hardware during production or distribution to make the end capability unstable. Alternatively, malware may also be introduced to create clandestine pathways into the capability's control systems. This would, if successful, allow the attacker to prevent the capability from operating either at will or through the occurrence of a pre-programmed event. In all, the overarching intent is to undermine the strategic relevance of a capability[676].

Though specifically demonstrated in the 2012 North Korean example, supply chain risks are recognised across numerous industries. This has led to the development of Supply Chain Risk Management (SCRM), a profession built around the aim of understanding, identifying, and reducing the risk of hostile actors targeting these processes [677]. Going further, industries have also recognised that with cyber threats forming a major element of supply chain risk,

[674] Greenert and Odierno, "Memorandum for the Secretary of Defense: Adjusting the Ballistic Missile Defense Strategy".
[675] Lewis and Unal, "Cyberattacks on Missile Systems".
[676] Ibid.
[677] A. Redondo et al., "Assessing Supply Chain Cyber Risks", *2019,* arXivLabs Cornell University (2019): 2.

a distinct sub-discipline of Cyber Supply Chain Risk Management (CSCRM) is also required[678].

Defined by Boyson as the assessment and mitigation of risks across the end-to-end processes of IT networks, hardware, and software systems, CSCRM has matured to be regulated by both industry and government standards[679]. Based on this, one might expect the ability of a state to launch left-of-launch cyber attacks against the air power supply chain to be limited. However, when examined, the reality is that states continue to actively target this area as a means of achieving effective left-of-launch cyber attacks.

A stark example of this was provided by a CISA Threat Alert (TA) published on 15 March 2018. In this, CISA confirmed that the Russian Government was actively targeting US Government and civilian contractors ranging from energy, through nuclear to aviation. Specifically, Russia's intent was identified as using cyber attacks against the US Government's supply chain which, according to the CISA, has less secure networks but still offers access to information and technology that could undermine air power[680]. With numerous links existing in this aerospace supply chain, it becomes evident that the area offers a rich environment to target left-of-launch cyber attacks against air power[681].

With numerous other examples of states conducting supply chain cyber attacks on the aviation industry being reported, it is necessary to consider whether this avenue could provide a means of impacting air power to a level at which it could

[678] For depth on CSCRM, see:
NIST, "Cyber Supply Chain Risk Management".

[679] For Boyson's assertion, see:
Boyson, "Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical It Systems", 342.
For representative standards, see:
NIST, "Framework for Improving Critical Infrastructure Cybersecurity", (National Institute of Standards and Technology 2018).
"Key Practices in Cyber Supply Chain Risk Management", (National Institute of Standards and Technology 2020).
UK, "Supply Chain Security Guidance ", ed. National Cyber Security Centre (2020).

[680] US, "Alert (Ta18-074a) - Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, 15 March (2018)", ed. the Office of the Director of National Intelligence (ODNI) and the National Security Agency (NSA) Cybersecurity and Infrastructure Security Agency (CISA) (2018).

[681] B. Prentice and P. Mee, "Aviation Industry May Be Vulnerable to Cyberattack through Its Global Supply Chain", *Forbes*, 11 April 2018.

lose strategic relevance[682]. In response, Oakley offers a scenario which, if realised, would confirm that it undoubtedly could[683].

Commenting in his analysis that the effect of malware introduced into the air power supply chain via cyber means could be as disastrous as any 'cyber Pearl Harbour', Oakley focuses on the risks surrounding logic bombs that might lie dormant for years [684]. When activated, either purposefully or through some form of pre-programmed trigger such as entering a designated area of air space, he suggests that the impacts could range from the loss of communications through to air platforms falling out of the sky. With the duration of the actual attack being momentary, a state would, in Oakley's scenario, not only be entirely blindsided but would lose air power as a strategically viable capability in a matter of seconds[685].

Given this assessment, it can be concluded that left-of-launch cyber attacks on the air power supply chain could be as impactful as the 2012 North Korean example was for missile defence. To this end, though no definitive examples of where strategic impact has occurred to air power are yet in the public domain, it is evident that states must work on the assumption that their adversaries could gain considerable advantage in state-on-state conflict through left-of-launch supply chain cyber attacks.

Space

[682] Other examples of states conducting supply chain attacks on the aviation industry, including elements which supply military aviation, include an alleged PRC state cyber attack on suppliers to Airbus and attacks on Lockheed-Martin. For depth, see:

CERT-EU, "Airbus Supply Chain Hacked in Cyberespionage Campaign", ed. Computer Emergency Response Team (CERT) (EU) (2019).
C. Hart, "Hackers Target Airbus Suppliers", *Supply Management,* (2019).
Gady, "New Snowdon Documents Reveal Chinese Behind F-35 Hack".
IATA, "Aviation Cyber Security", (International Air Transport Association 2020).

[683] J.G. Oakley, *Waging Cyber War: Technical Challenges and Operational Constraints* (New York: Apress, 2019), 90.

[684] A logic bomb is a form of malware that remains dormant until a specific condition is met. For analysis and depth on logic bombs, see:

I. Saeed, A. Selmat, and A. Abuagoub, "A Survey on Malware and Malware Detection Systems", *International Journal of Computer Applications,* (2013).
H. Agrawal et al., "Detecting Hidden Logic Bombs in Critical Infrastructure Software", *International Conference on Information Warfare and Security,* 1 (2012): 3.

[685] Oakley, *Waging Cyber War: Technical Challenges and Operational Constraints*, 90.

Turning to Lewis and Unal's second vector for a left-of-launch cyber attack, we encounter the concept of using cyber means to target space assets[686]. Though not directly impactful, such attacks could due to a reliance on space operations materially undermine the effectiveness of air power.

Though the digital capabilities which led to air power's reliance on space began to come into service in the 1980s, the modern level of dependency did not fully emerge until the First Gulf War in 1990-91. Described as an 'apotheosis of 20th century air power', the US led Coalition's harnessing of digital means during the conflict established a new hallmark for air power. Concurrently, however, it also proved a new level of dependency on space operations[687]. Growing from there, the world has in the 21st century entered a reality in which everything from air power's communications to navigation are reliant on satellites[688]. The result is that the loss or compromise of space support would undermine the strategic effectiveness of air power.

Taking kinetic effects as an example, air delivered Precision Guided Munitions (PGM) form the backbone of a modern air forces' ability to conduct strikes. Of the 19 main PGM variants currently in operation, 15 rely on satellites to guide them to their target[689]. Therefore, even if air platforms were able to take flight, an effective left-of-launch satellite cyber attack could prevent the delivery of most munitions. This would materially undermine the strategic viability of air power. It should therefore be asked whether cyber means can affect space operations to a level at which their support is denied.

Exploring this question, Harrison et al comment that though cyber attacks on space operations require a high degree of sophistication, they do not require significant resources. Making the option available to not only super and great

[686] Lewis and Unal, "Cyberattacks on Missile Systems".
[687] Mason, "The Air War in the Gulf", 225.
[688] EMEA, "Aviation: Satellite Services", ed. Middle East and Africa (EMEA) Satellite Operators Association (ESOA) Europe (2020).
[689] Perju identifies the main variants of air delivered PGM as being guided by either satellite technology, inertial (a navigation system using on board motion and rotational sensors), lasers, thermal or radar. Of these, 15 of the main variants of PGMs in use in 2019 were guided by satellite technology.
V. Perju, "Precision Guided Bombs: Analysis", *Revisita Militara,* 2, no. 22 (2019): 112.

states but also regional states or state-sponsored actors, the potential of cyber attacks in this area have been assessed as likely to grow[690].

Expanding on this, Harrison et al reflect on the potential avenues through which states could target space operations. Ranging from compromising digital uplinks, downlinks, and crosslinks to the targeting of on-board systems of the satellites themselves, they comment that targets are numerous. Going further, they also note that even in the context of a single target multiple attack options exist. For example, considering satellites alone, an attacker might choose to target anything from the data itself by inserting false or corrupted information to seizing control of a satellite through an attack on its command-and-control system. With all these elements intrinsic to supporting operations, the achievement of any would lead to an effective left-of-launch attack which, in turn, would prevent space operations from supporting air power[691].

Though seeking evidential examples to support this are given the limited information in the public domain problematic, reports since the mid-2000s not only indicate that such attacks are possible but that the PRC is actively pursuing them. An assertion supported by an expert witness giving testimony to the US Congress in 2017, it was claimed that the PRC already had 'the engineering and expertise…to develop counter space cyber weapons'[692].

Examining whether these claims are valid, analysis as early as 2007 suggests that the PRC were at that time successfully targeting US satellites. For example, in October 2007 and July 2008 cyber attacks linked to the PRC against the US Geological Survey's Lundsat satellite were reported to have caused approximately 12 minutes of communications interference[693]. Though on these occasions attackers did not gain control over the satellite, a later attack in 2014 would go further. In this circumstance a group linked to the PRC used a commercial satellite station in Spitsbergen, Norway, as a conduit to access a

[690] T. Harrison, K. Johnson, and T. G. Roberts, "Space Threat Assessment 2018", (Centre for Strategic and International Studies, 2018), 4.
[691] Ibid.
[692] D.D. Chen, "Opening Statement of Mr David D. Chen Independent Analyst: Hearing before the Us China Economic and Security Review", ed. US Congress (Economic and Security Review Commission, 2017), 75.
[693] Harrison, Johnson, and Roberts, "Space Threat Assessment 2018", 13.

digital uplink for the US National Aeronautics and Space Administration (NASA) Terra Earth observation satellite. In doing so, the group reportedly 'achieved all [the] steps required to command the satellite'[694]. However, according to a NASA spokesman, no commands were successfully sent during the attack[695].

Indicating both the PRC's intent and capability to target its adversaries' space-assets, it is unsurprising that further reporting in 2014 indicated that the activity is continuing. On this occasion a group linked to the PRC was reported to have attacked a US National Oceanographic and Atmospheric Administration's (NOAA) satellite. Providing information on weather systems which are critical to US military operations, the attack forced the NOAA to take down the system and stop transmitting satellite images for two days[696]. Though not actually gaining control of the satellite, one can extrapolate that if the NOAA services had been key to a planned air power operation it could have acted as an effective left-of-launch attack preventing the projection of air assets.

The above examples illustrate that the PRC has for over a decade developed its cyber capabilities to a point at which space-based assets can be effectively targeted. They also show that these means could disrupt military operations. It is therefore possible to conclude that even though such means have to date been limited to 'temporary disruptions and damage', they retain the potential to deliver effective left-of-launch cyber attacks on space-assets[697]. If achieved, such events would undermine the strategic effectiveness of air power.

Offering the advantage of being hard to detect due to an often-opaque difference in space operations between non-intentional malfunction and malicious effects, cyber attacks on space assets have been assessed by industry expert Pollpeter as the 'number one counter space-threat'[698]. Also, likely to become available to

[694] Chen, "Opening Statement of Mr David D. Chen Independent Analyst: Hearing before the Us China Economic and Security Review", 75.
[695] T. Perrotto, interview by J. Wolf, 28 October 2011.
[696] US, "Us China Economic and Security Review Commission: 2015 Report to Congress", ed. United States Congress (2015), 296.
[697] R.P. Rajagopalan, "Electronic and Cyber Warfare in Outer Space", (United Nations Institute for Disarmament Research, 2019), 1.
[698] K. Pollpeter, "Testimony before the Us China Economic and Security Review Commission: Hearing on China's Advanced Weapons", ed. Economic and Security Review Commission (2017), 18.

at least those in the Belfer Centre's 'Top 10' *Cyber Power Index*, it is concluded that cyber attacks on space operations are increasingly likely to feature in any intent to undermine the strategic effectiveness of an adversaries' air power[699].

Infrastructure

A final left-of-launch consideration is the infrastructure upon which air power relies to deliver effective operations. Defined in broad terms as the 'basic physical structures needed for the operation of an enterprise', air power is uniquely infrastructure reliant when compared to the domains of land and maritime[700].

Ranging from the most overt elements including runways and airfield lighting, to the equally important but less outwardly obvious requirements of fuels and power, the loss or compromise of any one element will quickly bring air operations to a halt[701]. This reality has been starkly illustrated with examples ranging from the Battle of Britain in 1940 which saw the German Luftwaffe seeking to deny the RAF vital airfield infrastructure, to the systematic destruction of Iraqi Air Force Bases in the First Gulf War in 1990-91[702]. In reflecting on these events, it is evident that when effectively conducted the destruction of an air force's infrastructure achieves a highly impactful left-of-launch disruptive effect against the projection of air power.

Though these examples illustrate the decisive effect of traditional kinetic capabilities on an adversary's infrastructure, a key contemporary concern has

[699] The Belfer Center's Cyber Power Index 2020 lists the top 10 cyber powers as the US, the PRC, the UK, Russia the Netherlands, France, Germany, Canada, Japan, and Australia. However, other states including North Korea are also believed to be investing in the ability to deliver this form of cyber attack.

Voo et al., "National Cyber Power Index 2020".

[700] UK, "Joint Tactics, Techniques and Procedures 4-05: Operational Infrastructure", ed. Ministry of Defence (Development, Concepts and Doctrine Centre (DCDC), 2012), 1-4.

[701] D.C. Ploeger et al., "Airport Cooperative Research Program (Acrp) Report 138: Aviation Infrastructure ", (Washington D. C.: Transportation Research Board, 2015), 4.

[702] In advance of the Battle of Britain in 1940 Hitler's Directive Number 16 in July 1940 laid plans for the invasion of Britain under Operation Sea Lion. This was followed in August 1940 by Directive Number 17 which ordered the Luftwaffe to overpower the RAF with 'all forces at its command…[primarily focusing on] their flying units, their ground installations and their supply organisations'. Directive 17 represented a classic left-of-launch infrastructure attack. For depth and analysis, see:

D.C. Dildy, "The Air Battle for England: The Truth Behind the Failure of the Luftwaffe's Counter-Air Campaign in 1940", *Air Power History*, no. Summer (2016).

H.R. Trevor-Roper, *Hitler's War Directives: 1939-1945* (London: Sidgwick and Jackson, 1964).

Lambeth, *The Winning of Air Supremacy in Operation Desert Storm* 3.

Staff-Writer, "The Gulf War: A Chronology", *Air Force Magazine,* (2001).

become the cyber threat. This is driven by the acknowledgement that modern aviation infrastructure, whether civilian or military, has become reliant on digitally enabled networked technologies. Identified by the International Civil Aviation Authority (ICAO) as spanning everything from airfield communications, through airfield lighting to fuels and power systems, there is an acceptance that a successful cyber attack on any one element could prevent the launching of air platforms[703]. Reflected in recent governmental strategy, there is a consensus that to assure the viability of air power this cyber threat must be recognised and managed[704].

Considering the forms these threats could take, the focus for not only air power but most digitised industries is an increasing reliance on the Industrial Internet of Things (IIoT) and CPS[705]. Forming a digital ecosystem, the IIoT offers an overarching concept which describes the use of numerous private and public networks to deliver hypoconnectivity[706]. Describing a level of digital capacity designed to exceed potential traffic-handling or bandwidth demands, hypoconnectivity delivers an exacting combination of high availability, low latency, and redundancies to assure the uninterrupted nature of digital support which enables aviation infrastructure[707].

In fulfilling this intent, the IIoT facilitates CPS. Defined in broad terms as physical devices which integrate sensing, computing, control, and networking into physical objects, they are in essence the output or physical realisation of the cyber domain. Ranging in form from the smart speaker in your home to SCADA systems

[703] ICAO, "Civil Aviation Cyber-Security ", (International Civil Aviation Authority 2020).

[704] For examples of Governmental strategies and managing the cyber threat to aviation, see:
UK, "Aviation Cyber Security Strategy: Moving Britain Ahead".
US, "National Strategy for Aviation Security of the United States of America", ed. President of the United States (2018).

[705] The IIoT is commonly associated with being the main driver behind the concept of Industry 4.0. An abbreviation for the Fourth Industrial Revolution, this highlights how digital technologies are now not only computerising industrial techniques but also interconnecting them to enhance performance. Though offering significant advantage, the loss or compromise of the digital links provided by the IIoT would lead to a loss of operations in those industries, including aviation, which have become reliant on them.
T. Masood and P. Sonntag, "Industry 4.0: Adoption Challenges and Benefits for Smes", *Computers in Industry,* 121 (2929).

[706] For further discussion on, and definitions of, hypoconnectivity, see:
ComputerWeekly.com, "What Is Hypoconnectivity?", https://www.computerweekly.com/news/2240100953/What-is-hyperconnectivity.
V. Ranadive, "Hypoconnectivity: The Future Is Now'", *Forbes*, 19 February 2013.

[707] Availability refers to the amount of time a digital system is available to the user and is usually measured as a percentage.
US, "Data Network Evaluation Criteria Handbook", ed. Federal Aviation Authority (2009).

that are embedded in virtually all industrial processes, CPS are now ever present. Within this, they are also relied on to facilitate the infrastructure that enables the projection of air power.

Even when the importance of the IIoT and CPS to air power's infrastructure are recognised, and robust cyber security measures are considered, their complexity means that hostile actors are offered numerous avenues through which to achieve disruptive effect. Discussed in depth by Ervural and Ervural, common threats which could in this vein impact air operations include DoS attacks in which a network is bombarded with enough fake messages that its capacity is exceeded, and it fails to function. A second common example offered by Ervural and Ervural is routing attacks in which routing information is altered so that information loops and error messages are generated preventing systems from operating effectively[708].

Though these options are possible in all circumstances, analysts continue to highlight that the increasing use of the public internet as a bearer for the IIoT, even when such communications are secured through encryption, increases the potential for cyber attack. One might assume that this issue is limited to the civilian rather than governmental or military sectors in which air power operates. However, as Libicki highlights, organisations including the US DoD recognise that the digital environment controlled by a state is relatively small[709]. With cyberspace consisting of multiple elements, the vast majority of which are within the publicly accessible internet, the likelihood of all air power related systems being maintained in classified and protected areas is non-existent[710]. This is especially true for infrastructures such as power and fuels which even for military purposes are routinely delivered by commercial third parties.

Though Libicki himself counters this by stating that sophisticated states will maintain their own vigorously defended communications links, he misses two key

[708] DoS and routing attacks are only 2 possible avenues identified by Ervural and Ervural. Others include transmission threats, data breaches and network congestion.
B.C. Ervural and B. Ervural, "Overview of Cyber Security in the Industry 4.0 Era," in *Industry 4.0: Managing the Digital Transformation* ed. A. Ustundag and Cevikcan. E. (Birmingham: Springer, 2019), 272.
[709] Libicki, "Cyberspace Is Not a Warfighting Domain", 326; ibid.
[710] Ibid., 326.

points[711]. First, any digital network with an external connection is vulnerable to attack. Though all, especially sophisticated military systems, will be protected by network security tools such as firewalls, Intrusion Detection Systems (IDS) and Virtual Private Networks (VPN) none are fool proof. As O'Raw and Laverty explain, when an attacker attempts to compromise any of these, they are attacking a device constructed by people from conventional hardware. Because of this, when the devices are extensively probed, it is likely that both human and technical vulnerabilities will be found[712]. Therefore, it can be concluded that where any external connection exists so too does the potential for a successful attack.

Though numerous manifestations of this reality can be cited, a significant example occurred in December 2020 when malware of Russian origin was found on the apparently secure systems of the US Energy Department. Also known to have impacted up to 18,000 other organisations operating the target SolarWinds software, it vividly illustrates O'Raw and Laverty's point that no matter how secure a system might claim to be a persistent cyber attacker remains able to compromise it[713]. As all air power infrastructure which utilises the IIoT has the external pathways which facilitate such exploitations, all are vulnerable to a left-of-launch cyber attack[714].

Beyond these interconnected systems, even the most classified and well protected of systems remain vulnerable to cyber attack. For example, in designing secure digital environments architects will routinely include means

[711] Ibid.

[712] J. O'Raw and D. Laverty, "Restricting Data Flows to Secure against Remote Attacks", in *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (2020), 2.

[713] The December 2020 attack on the US Energy Department is assessed to have been linked to a wider attack on SolarWinds. For depth and analysis on the attack, see:
BBC, "Us Cyber-Attack: Us Energy Department Confirms It Was Hit by Sunburst Attack", *BBC News Online*, 18 December 2020.
R. Brandom, "Solarwinds Hides List of High-Profile Customers after Devastating Hack", *The Verge,* (2020).
J. Tidy, "Solarwinds: Why the Sunburst Hack Is So Serious", *BBC News Online*, 16 December 2020.

[714] Another illustrative point which highlights the vulnerability of air power's digitally enabled infrastructure is the power sector. For depth, analysis, and examples, see:
M. Robinson, "The Scada Threat Landscape", in *1st International Symposium for ICS & SCADA Cyber Security Re* (2013), 36.
N. Kshetri and J. Voas, "Hacking Power Grids: A Current Problem", *Computer Fraud and Security,* 50, no. 2 (2017): 92.
G. Macola, "The Five Worst Cyber-Attacks against the Power Industry since 2014", *Power Technology*, 2 April 2020.

such as air gaps and data diodes[715]. Preventing any digital pathway into the system, these should logically avoid a cyber attack occurring. However, this assertion was infamously shown to be incorrect by the Stuxnet virus. First identified in 2010, Stuxnet, which is believed to have been created by the Israeli and US Governments, was found to have infected an air gapped system in an Iranian nuclear facility. Causing SCADA systems to malfunction, the virus significantly damaged the targeted processes. In doing so it proved that no matter how secure a network is it can never be fully protected from cyber attack[716].

Placed in the context of air power's infrastructure, this example adds weight to the conclusion that all systems which support its delivery are vulnerable to cyber attack. With states including not only Russia but the US and Israel showing an intent and capability to target infrastructure and undermine military capability, it is also logical to assume that both the capability and intent exist to target air power. As such, it can be concluded that as a left-of-launch attack vector within state-on-state conflict, the targeting of an air power's infrastructure is both viable and, in the right circumstances, likely.

Criticisms of Left-of-Launch

Though recognised as a significant development in missile defence, left-of-launch strategies have also been widely criticised. Largely driven by a recognition of real-world strategic limitations, their actual deployment is viewed by some as unlikely. This is because rather than being part of an escalatory strategy, left-of-launch relies on an adversary acting before a threat has been made. With the cyber elements of the concept requiring considerable pre-planning over months if not

[715] An air gap is the simplest and most obvious solution to delivering security to a digital network. Specifically, it relies on a system having no direct external connectivity and relying on the use of removable digital media (i.e., USB sticks, CDs, etc) to move information onto and off of the network. For definitions and examples, see:

Techopedia, "Air Gap ", https://www.techopedia.com/definition/17037/air-gap.

BAE, "Cybersecurity Products: Data Diode ", BAE Systems, https://www.baesystems.com/en/product/data-diode-solution.

[716] The Stuxnet virus, which was initially discovered in July 2010, targeted Siemens software in an Iranian nuclear facility. For detail, see:

Z. Sembiring, "Stuxnet Threat Analysis in Scada (Supervisory Control and Data Acquisition) and Plc (Programmable Logic Controller) Systems", *Journal of Computer Science, Information Technology and Telecommunications Engineering,* 1, no. 2 (2020): 97.

years, critics assert that their actual use becomes one of pre-emption not protection making them in most circumstances unviable[717].

Exploring this further, Panda argues that left-of-launch cyber capabilities are especially limited as a deterrence strategy. This is because all cyber weapons rely on the exploitation of capability gaps which are routinely 'one use' since their identification will lead to the defender patching the vulnerability. Therefore, Panda concludes, as key elements of deterrence are to ensure that an adversary is aware of a capability and that a state is willing to use it, cyber weapons have no value in the left-of-launch context[718].

Taken collectively, Lewis and Unal argue that in missile defence left-of-launch is a dangerous game in which a state may feel forced into using a capability in the fear that it will be undermined without their awareness by cyber means[719]. Leading to a potential 'asymmetrical power struggle' with false confidence in cyber weapons, the result could, Lewis and Unal conclude, cause false signalling and an increased likelihood of conflict[720].

Placing these views in the context of air power, all the criticisms and concerns can be seen to apply. For example, Panda's argument on 'one use weapons' applies equally to all cyber based scenarios making any use of cyber in a left-of-launch scenario potentially a single opportunity and therefore of limited value. Further, left-of-launch cyber strategies could also plausibly undermine current uses of air power which form fine balances of power in regions from the Baltics to the South China Sea[721]. If realised, left-of-launch cyber uses against air power might plausibly increase the chance of miscalculation and conflict rather than avoiding it. Given this, states might in their use of these strategies be cautioned to consider the consequences.

[717] For further discussion on criticisms which focus on the 'pre-emptions' vs 'protection' of left-of-launch cyber capabilities, see:

Ellison, "Left of Launch".
Futter, "The Dangers of Using Cyber Attacks to Counter Nuclear Threats".

[718] A. Panda, "North Korea, Us 'Left of Launch' Cyber Capabilities and Deterrence", *The Diplomat*, 6 December 2018.

[719] Lewis and Unal, "Cyberattacks on Missile Systems".

[720] Ibid.

[721] Futter, "The Dangers of Using Cyber Attacks to Counter Nuclear Threats".
Lewis and Unal, "Cyberattacks on Missile Systems".

Viability of Left-of-Launch

Though the above criticisms are acknowledged, left-of-launch cyber attacks whether used against the supply chain, space or supporting infrastructure offer a tempting and, importantly, deniable means to undermine the strategic viability of air power. With the effects already shown in missile defence, and the opportunities illustrated for air power, it can be assessed as plausible that such means have either already occurred without targeted states being aware or will be used to such effect in the future.

With the effect quite possibly too clandestine to identify, especially when targeted against aspects such as infrastructure, one could further argue that analysts will never fully identify whether air power has been impacted by these means at a strategic level. However, this could be countered by the argument that the undermining of air power to the point at which it cannot achieve key defence tasks remains effective whether the source is identified or not. To this end, analysts and security practitioners alike would be advised to closely consider these left-of-launch cyber threats which are assessed as having the potential to negatively affect a state's ability to project air power.

Will Cyber Threats Undermine the Strategic Relevance of Air Power?

Having explored the current and potential future nature of cyber threats, it is finally necessary to return to the question of whether these will undermine the strategic relevance of air power in state-on-state conflict. To do so, it is noted that in Rid's seminal 2012 article on the topic he argued that 'cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future'[722]. Reflecting on this, Rid's assertions could

[722] Rid, "Cyber War Will Not Take Place", 7.

lead this discussion to conclude that cyber threats have not evolved to the point at which they could meaningfully impact air power.

Whilst Rid is the most quoted academic source for such arguments, his views have been echoed by others[723]. The most notable example is found in the *Tallinn Manual* which concluded as of its publication in 2013 that no events had ever met the criteria of 'war' through cyber means. Though in drawing this conclusion the Manual acknowledged that the Stuxnet virus had come close, and Russia's 2007 use of cyber means to target Estonia was widely reported as an act of 'cyber war', neither achieved sufficient real-world impact to be considered an 'act of war'[724].

Given these assertions it could be concluded that cyber threats will never reach across the littoral space to the air domain and materially undermine the strategic relevance of air power. Though based on the cyber attacks experienced to date this argument might hold legitimacy, the potential scenarios explored in the above discussion indicate that such a conclusion is short sighted.

To begin this challenge, there is value in considering what would fulfil the criteria of 'cyber war'. Specifically, Rid argues, a cyber act must 'have the potential to be lethal, be instrumental and be political'[725]. Giving his definition depth and provenance, Rid signposts the writings of Clausewitz as the 'most concise concept of war'[726]. In these Clausewitz identifies three elements which must be met for an event to be considered an 'act of war'. First, an act must be violent. Second, an act must always force the enemy to accept one's will. Third, an act is always political[727].

Given these parameters, the question is posed as to whether the evolution of cyber threats into cyber attacks could ever allow a state to achieve an 'act of war' and, if so, whether the outcome of such events could materially undermine the strategic relevance of air power. In reviewing the discussions presented above, it

[723] Ibid.
[724] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* 215.
[725] Rid, "Cyber War Will Not Take Place", 8.
[726] Ibid.
[727] Clausewitz, *On War* 15.

is evident that to date Panetta's warning of a 'cyber Pearl Harbor' has not occurred[728]. However, it is also evident that despite being in development since the earliest days of digital processing, the concept of cyber remains emergent. Perpetually driven forward by Moore's Law, this creates a dual pronged reality. First, air power's reliance on digital technologies will continue to grow. Second, hostile actors will continue to seek the ability to deliver effective cyber threats designed to impact air power via both direct and indirect means.

When combined and placed in the context of the continued pre-eminence of air power, it becomes inevitable that when state-on-state conflict arises combatants will be motivated to find digital means to undermine an adversary's air power. Potentially violent in their use if attacks were to cause the loss of air platforms, and certainly designed to bend the will of an adversary and achieve political ends, the enactment of potential cyber threats would therefore meet the Clausewitzian criteria for war.

Though this conclusion is theoretically engaging, the hard truth is of more interest to states. Specifically, these developments will likely lead an adversary to actively use cyber vulnerabilities as avenues through which to realise cyber threats. In combination, a credible end state could be realised in which a state's ability to project air power is materially undermined through deniable and difficult to respond to digital means. In such circumstances, any state that has become reliant on air power, as was argued to be increasingly the case in the 'first cause', will not only struggle to thrive but even survive in the face of a credible and potentially devastating cyber risk to air power.

Conclusion

In developing the final of the thesis' three causes of cyber risk, this Chapter has explored the concept of cyber threats. Having initially introduced the discussion, the foundational sections opened with an examination of the evolution and diffusion of cyber power and influence. In this, the three Industrial Revolutions

[728] Panetta, "Panetta Warns of Dire Threat of Cyberattack on Us."

were outlined before noting that a fourth digitally inspired revolution would soon 'blur the lines between the physical, digital, and biological worlds'[729]. Making digital information a strategic resource, it was accepted that though the diffusing power of digital means had made 'the stage more crowded' the world remained dominated by states[730].

Having understood the evolution of digital technologies, the discussion next defined cyber power and influence. Exploring the challenges this creates Kuehl's argument that cyber power in isolation is largely unimportant was accepted[731]. Linking back to Hart's definition explored earlier in the thesis, it was acknowledged that it is only by harnessing cyber power to achieve credible real-world influence that digital means find their relevance[732]. The key question, the section concluded, was therefore whether cyber threats have developed to a point at which they might meaningfully impact air power.

Before addressing this question, a final foundational discussion focused on the environment in which cyber threats operate. Acknowledging the common usage of the environmental domains of land, maritime, air and space, the competing arguments as to whether cyber should be accepted as a fifth domain were explored. On balance, it was concluded that whilst its acceptance was justifiable it was also invasive of all the other domains. Therefore, in examining the cyber threat to air power, it was asserted that the focus must be on the 'cyber littorals' or, more specifically, where cyber power reaches beyond the digital domain creating influence in the physical world inhabited by the air domain[733].

Building on this conceptual discussion, it was next examined how these forces manifest themselves. Beginning with a review of the relevance of cyber in state-on-state conflict, it was accepted that despite post-Cold War arguments to the contrary, state-on-state conflict remains inevitable. Given this, it was established

[729] Schwab, *The Fourth Industrial Revolution* 99.
[730] Nye, *Cyber Power*, 1.
[731] Kuehl, "From Cyberspace to Cyber Power: Defining the Problem."
[732] Hart, "Three Approaches to the Measurement of Power in International Relations".
[733] The concept of cyber littorals is taken from:
Withers, "What Is the Utility of the Fifth Domain?", 133.

that the thesis must consider what form cyber threats might take and whether, when achieved, these will undermine the strategic relevance of air power.

Having delivered this foundational discussion, this question was first considered in the context of the current manifestation of cyber threats to air power[734]. Initially focusing on the origins of the cyber debate, most prominently Arquilla and Ronfeldt's 1993 article which offered predictions of an impending 'cyberwar', it was concluded that early digital skirmishes have trod a path between a Clausewitzian 'war-like' nature and a non-kinetic asymmetric quality. Though such hybrid-warfare was acknowledged as not being new, the digital means through which it is being pursued were identified as novel. Citing the Russian Gerasimov Doctrine as an example, it was concluded that events have shown that cyberwar is not only here but has undermined the strategic relevance of air power.

Countering this argument, the Chapter next highlighted that other recent examples of state-on-state conflict had proved the continued conventional relevance of air power. Using as examples the role of Turkish air power in the 2020 Azerbaijan and Armenia conflict and the dominance of conventional capabilities in Russia's 2022 invasion of Ukraine, the discussion noted that states have either chosen not to use effective cyber capabilities or such capabilities do not exist. In either circumstance, it was deduced that cyber threats are not yet advanced enough to undermine the relevance of air power.

Building on this interim conclusion, the potential future cyber threat to air power was explored next. Opening the discussion, it was noted that whilst there are no examples of air power being credibly threatened in state-on-state conflict, it does not mean that the technology to do so does not already exist or will not soon be available. To address this and consider whether air power could in the future be undermined through cyber threats, the issue was considered from two distinct perspectives.

[734] Arquilla and Ronfeldt, "Cyberwar Is Coming!", 144.

First, the potential of using existing or rerolled capabilities to directly target air platforms was explored. Looking broadly to do so, the discussion examined Israel's use of cyber to prevent Syrian air defences from operating in its 2007 air strike on a suspected nuclear facility. Identifying that the cyber threats which achieved this could provide a counter-air A2AD capability, the example was illustrated through a discussion of PRC expansionist tendencies. Specifically, it was noted how if harnessed these means could allow the PRC to achieve control of the air in the South and East China Seas.

In a second direct example, the discussion focused on the increased reliance on UAVs in state-on-state conflict and their susceptibility to cyber attack. Doing so through identifying likely attack vectors and offering examples, it was found that existing cyber threats to unmanned air power could, if re-purposed, undermine its strategic effectiveness.

Following a critical analysis of these arguments, it was identified that like many forms of state-on-state attack cybers potential direct success against air platforms depends on the ill-preparedness of the defender. Therefore, the key question identified was whether air power is being effectively defended.

Moving to the second distinct perspective, the Chapter considered indirect or left-of-launch attacks. Outlining how the concept emerged from the field of missile defence, it was noted that since 2012 the focus has been on 'full-spectrum' defences primarily using cyber threats. Arguing that the concept is easily transposable to air power, the discussion employed Lewis and Unal's assessment of potential left-of-launch cyber attacks on missile systems as illustrative examples of how air power could be impacted[735].

Focusing first on the supply chain, it was highlighted that cyber threats in this area have been a long-standing concern in many industries. Demonstrating the validity of these in aviation, the example of a 2018 CISA TA which identified Russian state nefarious cyber intent in the aviation supply chain was cited.

[735] Lewis and Unal, "Cyberattacks on Missile Systems".

Developed through a predictive case study of malware being introduced into the supply chain, it was concluded that states could gain considerable advantage in state-on-state conflict through left-of-launch supply chain cyber attacks on air power.

Next considering the cyber attack vector of space, air power's reliance on the support provided by space-based assets was highlighted. Ranging from navigation to the delivery of PGMs, it was identified that the loss or compromise of space-operations through cyber means would materially undermine air power's viability. Using the example of PRC attacks on US satellites dating back to 2007, it was concluded that a successful cyber attack on another state's space operations could decisively undermine the strategic viability of air power.

Finally, considering infrastructure, air power's unique level of reliance on this factor when compared to the other domains was noted. Building on this, it was highlighted that in the modern era infrastructure is itself reliant on digital technologies from the IIoT to CPS. When combined, the likelihood of air power being significantly disrupted through a cyber attack on its supporting infrastructure was laid bare. Given that even the most well protected digital systems remain vulnerable, it was concluded that as a left-of-launch vector the targeting of air power's infrastructure is both viable and, in the right circumstances, devastating.

Reviewing this discussion, criticisms of left-of-launch strategies were identified. However, on balance, the discussion identified the effectiveness and deniability of left-of-launch cyber attacks on air power. Based on this, it is highly likely that attempts will be made to use such options to undermine the strategic viability of air power in future state-on-state conflict.

Drawing the Chapter to a close, the discussion finally examined whether cyber threats are likely to undermine the strategic relevance of air power. Employing Rid's 2012 article and the 2013 *Tallinn Manual* as principal points of reference, it was initially concluded that no acts of 'cyber war' have either been, or are likely to be, experienced[736]. Therefore, it is unlikely that cyber threats will themselves materially undermine air power.

Countering this, however, it was noted that despite cyber attacks not being currently able to undermine air power, the concept remains emergent. Driven forward by Moore's Law, it was highlighted that a dual pronged reality is created: air power's reliance on digital technologies will grow whilst hostile actors concurrently seek the ability to deliver effective cyber threats to impact air power. Taken collectively, it was concluded, cyber attacks are not only likely to increase in importance but, in due course, will inevitably meet the Clausewitzian criteria for war.

Building on this, the realities of this theoretical discussion were finally explored. Specifically, with adversaries likely to use cyber vulnerabilities as avenues through which to realise the cyber threats introduced above, the combination will create an undermining of the ability to project air power. In such circumstances, any state that is reliant on air power will struggle to not only thrive but even survive in the face of a credible cyber risk.

In bringing this and the wider discussion on the three causes of air power's cyber risk to a close, it is noted that the conclusions present a stark reality for states in the digital age. Specifically, states are increasingly reliant on digitally enabled air power to maintain their role but, through a combination of cyber vulnerabilities and threats, this capability is at credible risk of being lost or compromised via cyber means.

However, as with any theoretical discussion it must, to be valid, be tested if the cyber risk to air power is to be accurately assessed. To achieve this, Part 3 of the thesis will use the cyber risk to Western air power as a vehicle to explore the topic. Delivered through three case study-based chapters, this will explore the cyber vulnerabilities of Western air power, the cyber threat posed to Western air

[736] Rid, "Cyber War Will Not Take Place", 57.
Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* 215.

power and, finally, an examination of the overall cyber risk through three representative scenarios. In doing so, the Part will not only establish the validity of the above conclusion but expose whether the cyber risk to air power, and the affect it has on a state's role, is absolute affecting all equally, or relative with some likely to be more impacted than others.

Part 3: The Consequences of Air Power’s Cyber Risk (A Case Study of Western and Aligned States)

Chapter 7: The Cyber Vulnerabilities of Western Air Power

Introduction

Building on Part 2's examination of the 3 causes of air power's cyber risk, Part 3 will test the validity of the conclusions. Acknowledging the scope of the topic, and the restrictions of the thesis, this will be achieved through a case study pragmatically narrowed to Western and aligned states. Employing this sub-set of the international community as a manageable focus through which discussion on the consequences of air power's cyber risk can be developed, conclusions applicable on a global scale will be drawn and crystallised in the concluding discussion presented in Part 4 of the thesis.

Opening the discussion, this initial Chapter of Part 3 examines cyber vulnerabilities through three representative lenses: the US as a superpower, the UK as a great power and Taiwan as a regional power. Adopting a common analytical structure throughout, the discussion will in context of history, contemporary position, and military power lead to an examination of their respective air power cyber vulnerabilities.

Reviewing all three representative states in a concluding section, two consistent themes will be identified. Firstly, all current air platforms, whether cutting edge fifth-generation or iteratively developed fourth-generation, are susceptible to cyber vulnerabilities. Secondly, though air platforms themselves may be the natural focus of this discussion, it is the wide-ranging left-of-launch concerns which will be found to represent the most impactful cyber vulnerabilities. Developing these assertions, it will be concluded that the reality for all air forces is that due to ingrained cyber vulnerabilities, the cyber domain may be where conflicts are won or lost.

Though important for all, it will finally be argued that the impact of cyber vulnerabilities is inverse to the size of the state. With superpowers more insulated due to their breadth of capabilities they are likely to maintain their role despite cyber vulnerabilities. For great states this becomes more concerning with cyber vulnerabilities able to undermine limited mass and challenge the maintenance of their role. Whilst concerning for great states, it will finally be judged that the issue gains existential proportions for regional powers faced with aggressive neighbours. In these circumstances, cyber vulnerabilities may, if exploited, remove a key air power deterrence, and shift the strategic calculus. Increasing the likelihood of potential aggression, the result may be disastrous. However, to judge the full cyber risk, the intent and capability of those threat-actors that may exploit the vulnerabilities must be known. It is this complementary factor that will be addressed in Chapter 7.

United States (US): Superpower

Introduction to US Air power’s Cyber Vulnerabilities

To consider the cyber vulnerabilities to US air power, this section will explore the nations’ role in a realist-constructivist world. Doing so by tracking its development from the Cold War through to contemporary great power competition and overlaying this with an exploration of military and air power specific capabilities, the section will move towards a final discussion of US air power’s cyber vulnerabilities.

Exploring this area through the lenses of direct, left-of-launch and espionage related cyber vulnerabilities, it will be asserted that the US could, via cyber, lose its strategic advantage. From this, it will ultimately be concluded that a concerning picture of a superpower struggling to maintain its self-conceived exceptional role has emerged. With air power’s cyber vulnerabilities identified as a potential ‘Achilles heel’ that may expedite this concern, it will be asserted that counterbalancing these must, for the US, be a priority.

The US: Through Bipolar to Unipolar and Towards Uncertainty

To understand the position and role of the US in the contemporary realist-constructivist world, the most intuitive route is to explore its development through three distinct phases: a bipolar Cold War, a unipolar post-Cold War and an uncertain future in which the US faces a resurgent Russia and a PRC on the cusp of superpower status[737]. Running as a theme through these, the discussion must also acknowledge the continuing influence of US strategic culture[738]. Pivoting around the precepts of the Monroe Doctrine and geographical realities, their guiding hands can be seen in both historic US 'isolationism' but, more germane to this discussion, its conceptualisation as an 'exceptional' power, set aside from others and able to act unilaterally to achieve its aims[739]. To explore how these have combined there is value in stepping back and considering the US from the Cold War onwards.

Approached from a constructivist perspective, the Cold War period is characterised by Hopf as defined by strong Western and Eastern sociocultural identities which produced fundamental understandings and an ultimate divide between the US and Soviet Union[740]. From the US perspective, these identities were founded on the long-lasting influence of the Monroe Doctrine but reinforced by individualistic and liberal values evolved from a lack of European social

[737] For depth on bipolarity, see:
B. Buzan, Wæver, O., Regions and Powers: The Structure of International Security (Cambridge: Cambridge University Press 2003).
For depth on unipolarity, see:
C. Krauthammer, "The Unipolar Moment", *Foreign Affairs* 70, no. 1 (1991).
C. Krauthammer, "The Unipolar Moment Revisited", *The National Interest,* (2003).

[738] The term 'strategic culture' was first coined by Snyder in a 1977 RAND report. For the report and further depth, see:
J. L. Snyder, "The Soviet Strategic Culture: Implications for Limited Nuclear Operations", (RAND, 1977).
Al Rodhanm R.F., "U.S. Space Policy and Strategic Culture", *Journal of Interational Affairs,* (2018).
C. S. Grey, *Modern Strategy* (Oxford: Oxford University Press, 1999), 5.
For assessments on the static nature of the US strategic culture, see:
N. Al Rodhan, "Strategic Culture and Pragmatic National Interest", *Global Policy,* (2015).
T.G. Mahnken, "United States Strategic Culture", (Advanced Systems and Concepts Office: Defense Threat Reduction Agency, 2006), 3.
L Varadarajan, "Constructivism, Identity and Neoliberal (in)Security", *Review of International Studies* 30 (2004): 320.

[739] The Monroe Doctrine first articulated in 1823 by US President James Monroe in an address to the US Congress set out 3 basic precepts: to maintain separate spheres of influence, non-colonisation, and non-intervention. For depth on the Monroe Doctrine, its impact and development over time, see:
US, "Monroe Doctrine, 1823", ed. Office of the Historian (2022).
Al Rodhan, "Strategic Culture and Pragmatic National Interest".
Mahnken, "United States Strategic Culture", 5.
For comment on how the Monroe Doctrine has developed into US 'exceptionalism', see:
C Vann Woodward, "The Age of Reinterpretation", *American Historical Review* 66 (1960): 6.
W. Lippmann, *Public Opinion and Foreign Policy in the United States* (London: Allen and Unwin, 1952), 25.

[740] T. Hopf, "The Promise of Constructivism in International Relations Theory", *International Security,* 23, no. 1 (1998).

hierarchies[741]. Collectively, this created a US identity which defined the world not as economic communities or former colonies but battlegrounds in which it must protect against the antithesis of liberal democracy, communism[742].

Operating against this backdrop, the US became balanced against the Soviet Union not through wider conceptualisations but because of the singular communist identity[743]. With this stark divide underpinned by the 'tense and dynamic period' of high-stakes thermonuclear competition, the breeding ground for the US's self-defined 'exceptionalism' was established. In this, the US came to adopt an enduring perception of itself as aside from, or even above, all other states[744].

Entrenched for nearly half a century, this Cold War reality would only materially shift in 1991 following the collapse of the Soviet Union. Characterised by many IR scholars as a 'grand strategic opportunity for countries to reflect on their past, present and future', the period saw in a constructivist sense the opportunity for a significant revision of roles[745]. However, for the US this would be played out not in a shift of role or strategic culture, but in a growth of exceptionalism as it asserted itself to be the sole surviving superpower against a diminished Russia and yet to be emergent PRC[746].

Aligned to this, the US would, without a major state adversary, also transition its export of liberal democracy from a state-centric to concept-centric approach. Illustrated by an increase in US-led collective security rules, it focused on themes including punishing the proliferation of Weapons of Mass Destruction (WMD) to states that did not support its ideals, countering terrorism where it was levied against liberal democracies and addressing human rights abuses when committed by authoritarian regimes with whom it was not aligned.

[741] For the evolution of US liberal values, see:
Al Rodhan, "Strategic Culture and Pragmatic National Interest".
For the US perceived right to reform the international system, see:
Mahnken, "United States Strategic Culture", 6.
[742] Hopf, "The Promise of Constructivism in International Relations Theory".
[743] Ibid.
[744] D. Pierce, "America in the Post War Period", *Inquiries* 1, no. 10 (2009,).
[745] J.S. Lantis, "Strategic Culture and National Security Policy", *International Studies Review,* 4, no. 3 (2002): 88.
[746] Ibid., 89.

Exploring this period, Frederking highlights how both Kosovo and Iraq act as examples of the shift. Though acknowledging differences including Kosovo's focus on human rights and Iraq's focus on proliferation, at a pragmatic level he argues that the two have 'stunning similarities' in terms of US motivation and strategic culture. Firstly, in both there were disputes on how to implement collective security rules with the US advocating for force, and Russia and the PRC advocating for weapons inspections. Secondly, there was debate on whether force would achieve the invocation of collective security rules with the US asserting they would, and Russia and the PRC arguing that without UNSC authority any force would violate international law. Whilst in both the ultimate success of subsequent actions can be debated, their occurrence under US-led coalitions against global resistance highlights a level of unrivalled power applied in a period when US strategic culture set the direction for world events[747].

With this argument further supported by the prevalence in the 1990s and early 2000s of US led or inspired concepts including the 'Clinton Doctrine' and R2P, a 'unipolar moment' in history is unveiled[748]. In this, critics of the US argue that rather than being positive, the 'Clinton Doctrine' and R2P were 'Trojan Horses' designed to legitimise US-led Western interventions. Though benefiting some, when considered more widely, these critics conclude that when suffering did not coincide with US interests any supposed responsibility to protect was ignored[749].

[747] For Frederking's arguments, see:
B. Frederking, " Constructing Post-Cold War Collective Security", *American Political Science Review,* 97 (2003): 363.

[748] Named after US President Bill Clinton, the 'Clinton Doctrine' focused on the use of force to protect democratic principles as defined by the US version of liberal democracy. For depth, see:
D. Brinkley, "Democratic Enlargement: The Clinton Doctrine", *Foreign Policy,* 106 (1997).
P. Clawson, "The Clinton Doctrine", *The Washington Institute for Near East Policy,* December (1997).
For depth on this period as a 'unipolar moment' in history, see:
Krauthammer, "The Unipolar Moment".
Krauthammer, "The Unipolar Moment Revisited".

[749] For arguments on the use of R2P and other means as a 'trojan horse' (and similar metaphors), see:
R.W Murray, "Intervention in the Emerging Multipolar System: Why R2p Will Miss the Unipolar Moment", *Journal of Intervention and Statebuilding* 6, no. 4 (2013).
C. Focarelli, "The Responsibility to Protect Doctrine and Humanitarian Intervention: Too Many Ambiguities for a Working Doctrine", *Journal of Conflict and Security Law,* 13, no. 2 (2008).
R. Hoa, "Rhetoric of Responsibility: R2p's Harmful Application in Humanitarian Practice", *E-International Relations* (2015).

Though distinct, this period of US unipolarity would from the early 2000s show signs of erosion[750]. The first event to signal this was 9/11[751]. Causing a dramatic review of the threats posed to the US and how these might be managed, 9/11 shifted the US away from founding their actions on concepts such as R2P to openly using force in targeting adversaries[752]. Emerging as the 'Global War on Terror', a nexus between international terrorism, weapons of mass destruction and 'states of concern' was created which, in combination, were used to legitimise US actions. These were designed to defend its role as a global superpower with self-defined exceptional rights to act[753].

With this foundation formalised in the 2002 National Security Strategy (NSS), the US officially set out how it would act against its challengers to retain its presupposed rights[754]. Though not altering the essence of US strategic culture or its role, both of which coalesced around defending and exporting its version of liberal democracy, the NSS did confirm the dramatic post 9/11 changes[755].

A notable illustration of this was the 2003 Gulf War. Though for some constructivists this US-led invasion of Iraq signified a shift in US strategic culture, the reality was that US national identity remained unchanged[756]. Contouring the post-9/11 nexus and the NSS's identification of new threats, the actions showed how the US viewed itself as a benevolent nation using force to defeat the twin ideological threats of 'rogue states' and militant Islamic fundamentalism[757]. Though in doing so the US amended its rhetoric, the overarching strategic culture and role remained consistent. Reinforced by key members of the Bush Administration through concepts including the 'one percent doctrine' and

[750] J.L. Gaddis, "Toward the Post-Cold War World ", *Council on Foreign Relations,* 70, no. 2 (1991): 103.
[751] For detail on the events of 9/11, see:
9/11 Commission, "The 9/11 Commission Report ", (National Commission on Terrorist Acts Upon the United States 2004).
[752] W. Mirow, *Strategic Culture, Securitisation and the Use of Force: Post-9/11 Security Practices of Liberal Democracies* (London: Routledge, 2016), 3.
[753] W. Aldrich Rees, R.J., "Contending Cultures of Counterterrorism: Transatlantic Divergence or Convergence", *International Affairs* 81, no. 5 (2005): 906.
[754] US, "The National Security Strategy", ed. National Security Council (2002).
[755] Varadarajan, "Constructivism, Identity and Neoliberal (in)Security", 320.
[756] For the constructivist assessment on a change in strategic culture through the Iraq War, see:
T. Lauterbach, "Constructivism, Strategic Culture, and the Iraq War", *ASPJ Africa & Francophonie,* (2011): 63.
[757] A. Flibbert, " The Road to Baghdad: Ideas and Intellectuals in Explanations of the Iraq War", *Security Studies* 15, no. 2 (2006): 331.

'demonstration effect', the groundwork was set for a continuation of US behaviours under a new structure of legitimisation[758].

Though 9/11 and the events in Iraq are notable for the post-Cold War period, arguably the most significant event which will define the future manifestation of US identity and role is the rise of the PRC. Threatening the US for the first time since 1991 with the spectre of a near-peer competitor, this has caused the US to engage in an overt 'pivot to Asia'[759]. Though significant in terms of policy and positioning, Harris argues that the pivot reflects a 'historical continuity' in US role and strategic culture rather than any major change in strategic calculus[760].

Allowed by a decline in US commitments in Iraq and Afghanistan, and driven by President Obama's recognition that the world's most populous region will become the epicentre of 21st century global affairs, this 'pivot' is in Harris's logic a simple re-balancing of US resources. In this, the US will seek to maintain its global position and reinforce the influence of liberal democracy[761]. Viewed in these terms, the 'pivot' is yet another example of US exceptionalism exerting a perceived right to globally project against any force, whether state or ideology, which might challenge it.

[758] Key members of the Bush Administration who supported this direction included President G.W. Bush, Vice-President Dick Cheney, Secretary of Defence Donald Rumsfeld, and National Security Advisor Condoleezza Rice. For comment on their role, see:

T.E. Ricks, *Fiasco: The American Military Adventure in Iraq* (New York: Penguin Press, 2006), 27.

The 'one percent chance' refers to Vice-President Cheney's position that if there was a 'one percent chance' of Iraq possessing, using, or threatening the use of nuclear weapons to constrain US freedom of action then the US must act against it. For depth on this concept, see:

R. Suskind, *The One Percent Doctrine: Deep inside America's Pursuit of Its Enemies since 9/11* (New York: Simon & Schuster, 2006).

The 'demonstration effect' refers to Vice-President Cheney's view that the military invasion of Iraq was a lesson to other regimes not to threaten US interests. For depth on Iraq and the demonstration effect, see:

A.I. Butt, "Why Did the United States Invade Iraq in 2003?", *Security Studies,,* 28, no. 2 (2019): 273.

[759] For analysis of the US not facing a near-peer competitor since the Cold War, see:

B.F. Harris, "United States Strategic Culture and Asia-Pacific Security", *Contemporary Security Policy,* 35, no. 2 (2014): 291.

For predictions on the speed of the PRC rise, see:

US, "Global Trends 2030: Alternative Worlds", ed. National Intelligence Council (2012), iii.

[760] For an analysis of President Obama's recognition of the PRC threat, see:

K.G. Lieberthal, "The American Pivot to Asia ", *Brooking Institute,* (2011).

For Harris's assessment, see:

Harris, "United States Strategic Culture and Asia-Pacific Security", 299.

[761] For discussion on President Obama's recognition of the importance of the Asia-Pacific, see:

Lieberthal, "The American Pivot to Asia ".

For a discussion on the rebalancing of US resources to meet this recognition, see:

P. Birgbauer, "The Us Pivot to Asia Was Dead on Arrival ", *The Diplomat,* (2022).

Finally moving to the two most recent administrations of Presidents Trump and Biden, further evidence of the unwavering nature of US strategic culture, role and identity is offered. Though from Obama through Trump to Biden the pendulum of political views and rhetoric swung significantly, the fundamental direction of the US remained surprisingly constant. In relation to the PRC, for example, the 'pivot to Asia' was retained under Trump through economic tariffs[762]. Transitioning into the Biden administration, this continued. Despite taking a different tact by embracing the alliances Trump had rejected, Biden continued to hold Asia as a strategic priority underlined by a 'muscular posture' towards the PRC[763].

Considered collectively, the above narrative illustrates an overarching US strategic culture, role and identity which have remained unchanged from the 1950s. Specifically, the US continues to position itself as a global superpower with the exceptional right to not only export and enforce liberal democracy but do so unilaterally with or without allies as the situation dictates. Looking forward, the emergent issue for the US is whether with a growing PRC and an assertive Russia it will by the middle of the 21st century have the power and influence to maintain this role[764]. Though such issues must in their totality be addressed across all the levers of national power, for a state so used to using force to support its strategic aims, the question is whether the US has the military power to meet the challenge.

The US Military Instrument: Failing the Two Major Regional Conflict (MRC) Requirement

In this role as a superpower seeking to guarantee liberal democracy, the US military instrument has by necessity extended beyond defending its own country to globally defending the principles central to its self-conceptualisation. Entwined

[762] "The Us Pivot to Asia Was Dead on Arrival ".

[763] Ibid.

[764] For comment on this shift away from US unipolarity and the PRC / Russia challenge, see:
US, "Renewed Great Power Competition: Implications for Defense—Issues for Congress", ed. Congressional Research Service (2022).
M.N Katz, "Great Power Clashes Will Reshapte America ", *National Interest,* (2021).
T. Wright, "Putin Is Taking a Huge Gamble", *Brooking Institute,* (2021).
H. Brands, "The Eurasian Nightmare: Chinese-Russian Convergence and the Future of American Order", *Foreign Affairs,* (2022).

with its sense of exceptionalism, the drive has translated into both deterring and using reactive force to control global adversaries[765]. In considering the challenges this poses, commentators point out that despite its military might translating power into global military dominance in a new era of great power competition is increasingly uncertain[766]. To explore this in more depth, and consider whether for the US it is achievable, two simple but informative metrics are budgets and people.

In terms of the first, the US has by a considerable margin the world's largest military budget with in 2020 it equating to 39 percent of worldwide defence spending. Though against other metrics such as spending as a percentage of GDP this is lower than states including Saudi Arabia, Israel, and Russia, the sheer scale of the US economy places its financial commitment in an unassailable position[767]. Already three times larger than that of the PRC, and predicted to increase until at least 2031, one might expect the US to have both the power and dominance to achieve its strategic intent[768].

Translated into numbers of military personnel, this expectation continues. Though far below its Second World War peak of over 12 million, the US has for the last 70 years maintained a large standing force. Admittedly fluctuating as a reflection of strategic challenges, it has never fallen below 1.3 million even in the post-Cold War 1990s[769]. Whilst one could argue that this number is dwarfed by its adversaries with the PRC maintaining over 2 million and Russia over one million,

[765] This characterisation of the role of the US armed forces is taken from:
Staff Writer, "Introduction: An Assessment of U.S. Military Power", *Heritage Foundation,* (2021).

[766] For a specific discussion on US military power 'vs' US global military dominance, see:
J. Lynch, "The Myth of American Military Dominance", *War on the Rocks* (2019).
For commentary on the possible shortfalls of contemporary US capability in the face of multiple threats, see:
Watts. S., "A More Peaceful World? Regional Conflict Trends and Us Defnece Planning ", (RAND 2017).
Writer, "Introduction: An Assessment of U.S. Military Power".

[767] M. Szmigiera, "Countries with the Highest Military Spending 2020", (Statistica, 2021).

[768] For predictions of the future US defence budget out to 2031, see:
E. Duffin, "U.S. Defense Outlays and Forecast 2000-2031", (Statistica, 2021).For detail on the NDAA, see:
For detail on the most recent US defence budget, the National Defense Authorisation Act (NDAA), see:
US, "National Defense Authorization Act for Fiscal Year 2022", ed. US Congress (2021).
Staff Writer, "Biden Signs Enormous Us Military Budget into Law", *Al Jazeera*, 27 December 2021.
For detail on bipartisan support for the NDAA, see:
J. Reed, "Senate Passage of National Defense Authorization Act for Fiscal Year 2022," news release, 15 December 2021, https://www.armed-services.senate.gov/press-releases/reed-inhofe-praise-senate-passage-of-national-defense-authorization-act-for-fiscal-year-2022
J. Inhofe, "Praise Senate Passage of National Defense Authorization Act for Fiscal Year 2022", news release, 15 December, 2021, https://www.armed-services.senate.gov/press-releases/reed-inhofe-praise-senate-passage-of-national-defense-authorization-act-for-fiscal-year-2022.

[769] D. Coleman, 2021, https://historyinpieces.com/research/us-military-personnel-1954-2014.

other US advantages balance pure numbers[770]. For example, though its exceptionalism sees it aspire to act unilaterally, the US's wider NATO alliance allows it to call on nearly 3.5 million personnel[771]. Furthermore, by harnessing technology the US has reduced its requirement on sheer mass[772]. Given these factors, the US should, even when outnumbered, deliver the level of combat power required to meet its strategic intent.

Taken in these terms, the US military appears able to support the US role. However, with the art of military success not founded on money, people, or capabilities, but identifying and understanding adversaries, such metrics in isolation lack context. For the US the question is therefore not whether it has enough people and money, but whether it has the correct capabilities and doctrine to employ these resources effectively in an era of great power competition.

When reflecting on how the US has approached this challenge, especially since the loss of clarity offered by the bi-polar Cold War, an informative starting point is the 1993 Bottom-Up Review (BUR). Led by Les Aspin, US Secretary of Defense, the BUR recognised both the dramatic changes brought about by the end of the Cold War and how these altered US security needs[773]. Building on this, the BUR argued that the US must reassess defence concepts, plans, and programs 'from the ground up' with a focus on simultaneously pursuing two regional conflicts[774]. The legacy of this decision, and the US choice to adopt it, created an enduring 'two-MRC' standard which in today's great power competition has renewed resonance.

Whilst significant, the BUR was reconsidered by successive US administrations. Most notably challenged by the US Quadrennial Defense Reviews (QDR)

[770] N. Routley, "Mapped: All the World's Military Personnel", (Visual Capitalist 2022); NATO, "The Power of Nato's Military", ed. NATO Newsroom (2022).
[771] "The Power of Nato's Military".
[772] Examples of technology replacing mass include the US Army which by 2019 through technology supported economies of scale reduced to 420,000 personnel and future developments including Robotic Combat Vehicles (RCV) which aim to go further. For depth on these developments, see:
E. Ackerman, "U.S. Army Considers Replacing Thousands of Soldiers with Robots", *IEEE Spectrum,* (2014).
K. Osborn, "The U.S. Army's Future: All About Robots?", *National Interest,* (2021).
[773] L. Aspin, "Report on the Bottom-up Review", ed. Department of Defence (1993), 3.
[774] Ibid.

conducted from 1997 to 2014, these, despite being modelled on the BUR, shifted focus from operational to institutional issues[775]. In doing so they lost sight of military necessities, became obsessed with metrics and, ultimately, undermined the 'two-MRC' standard. As a result, the US armed forces came in danger of being unable to effectively deliver against the US strategic role[776].

Replacing the QDR in 2018, the National Defense Strategy (NDS) which was built on an independent US DoD Commission took a different tact[777]. No longer focusing on metrics but security challenges, the Commission moved the US armed forces back towards operationally focused delivery[778]. Notably, it recognised the increasing global pressures of the PRC in the Indo-Pacific, Russia in Europe, and ISIS in the Middle East[779]. To face these, the Commission argued that the US needed a larger force than it had in 2018. With air power at the forefront of its domain focused recommendations, the Commission specifically stated that to face either the PRC, Russia, or ISIS the US needed more stealthy long-range fighters, air-to-air tankers, air transport and ISR platforms. To face all concurrently, and meet the 'two-MRC' standard, it concluded that the US military needed significant capability uplifts across the board[780].

With increases in global power competition since 2018 supporting the Commission's conclusions, it is evident that to achieve the US chosen role its armed forces must re-embrace the 'two-MRC' standard and grow capabilities to match. Though to date the Biden Administration has not replaced the NDS, its Interim National Security Strategic Guidance (INSSG) echoes these conclusions. Of note, in discussing the roots of the US national security requirement, the INSSG confirms that it needs to 'deter and prevent adversaries from directly

[775] For detail on the QDR's, see:
US, "Quadrennial Defense Review", ed. Historical Office of the Secretary of Defense (2022).
For the assessment of the QDR's, see:
J Schrader, Y. , L. Lewis, and R.A. Brown, "Quadrennial Defence Review (Qdr) Analysis: A Retrospective Look at Joint Staff Participation ", (RAND 1999).
[776] Writer, "Introduction: An Assessment of U.S. Military Power".
[777] US, "National Defence Strategy of the United States of America ", (2018).
[778] "Providing for the Common Defense", ed. National Defense Strategy Commission (2018).
[779] Ibid., 35.
[780] Ibid., 36.

threatening the US and our allies, inhibiting access to the global commons, or dominating key regions'[781].

Based on this, it can be concluded that the US has recognised that despite maintaining a large military, its armed forces are not aligned to achieving the unilateral multi-front activity demanded of a superpower with exceptional expectations in today's world of great power competition. Considered in this context, and acknowledging the 2018 Commissions focus on air power, it is necessary to explore how the air domain plays into this conclusion and how it might rebalance the strategic scales.

US Air Power: No Longer Exquisite

Writing in 2020, USAF Chief of Staff General Charles Brown commented that in an environment defined by 'declining resources, aggressive global competitors, and rapid technology development and diffusion', US air power must accelerate change to underwrite the level of national security expected of it[782]. Through this, Brown is acknowledging how the above conclusions on US military power are reflected in air power's contemporary reality. Specifically, the US constructivist identity of an exceptional state able to project global power at will was exemplified in a late 20th century 'historically-anomalous period' of air power dominance in which its land and naval forces could operate unthreatened from the skies[783]. However, with the world in the third decade of the 21st century, and the US facing growing peer-competitors, it has been reminded that neither air dominance nor the ability to act uncontested are US birth rights[784].

The impact of this is a recognition that to maintain its role the US must revolutionise its' air power, with the vehicle intended to achieve this being the Air Force Future Operating Concept (AFFOC)[785]. Setting out the future strategic context, the AFFOC states that the nation will 'employ advanced technology in

[781] US, "Interim National Security Strategic Guidance ", ed. White House (2021), 9.
[782] C.Q. Brown, "Accelerate Change or Lose ", (United States Air Force 2020), 3.
[783] Ibid.
[784] Ibid.
[785] US, "Air Force Furute Operating Concept: A View of the Air Force in 2035", ed. US Air Force (2015).

innovative ways to deter and defeat adversaries'[786]. Also emphasising that the nature of warfare will remain unchanged through to 2035, its' keystone ideas focus on the delivery of uncontested global vigilance, reach, and power in the air domain[787]. To achieve these, the US intends to maintain multiple operational options to seize and retain the air initiative. Likened to placing an adversary on the 'horns of multiple dilemmas', this would move the US away from a singular focus on exquisite platforms to embracing an ability to deliver 'flexibility, speed, coordination, balance, and strength'[788].

In exploring this proposal, a 2020 RAND report assesses that the AFFOC, like all US strategic doctrine, is unlikely to accurately predict the future of warfare[789]. This sentiment was underlined by Robert Gates, US Secretary of Defence, who in 2011 asserted that 'when it comes to predicting the nature and location of our next military engagement…we have never once gotten it right'[790]. Through this, a clear note of caution is raised over whether the intended transformation of air power can be successful.

Counterbalancing this, however, all military strategists accept that given the long lead-in time for the delivery of air power, predictions, even if imperfect, must be made. This reality and the aspiration which underpins AFFOC were encapsulated by General Martin Dempsey, Chairman of the US Joint Chiefs of Staff, who using a sporting analogy said that the US must 'skate to where the puck is going to be, not where it's been'. By doing this, he concluded, US air power will be decisive in future conflicts[791].

Exploring the future structure of US air power through these conclusions, RAND asserts that the 'puck' is likely by 2030 to be spread across four diverse types of conflict with each demanding a different suite of capabilities. If all cannot be addressed concurrently, RAND argues that the US will 'progressively lose the

[786] Ibid., 5.

[787] In full, the US's doctrinal 5 core missions of air power are: air and space superiority, Intelligence, Surveillance and Reconnaissance (ISR), rapid global mobility, global strike, and Command and Control (C2). For depth, see:
US, "Global Vigilance, Global Reach, Global Power for America", ed. US Air Force (2013).

[788] "Air Force Furute Operating Concept: A View of the Air Force in 2035", 11.

[789] R.S. Cohen, "The Future of Warfare in 2030", (RAND, 2020), ix.

[790] R. Gates, "Speech to the Us Military Academy, West Point ", ed. US Department of Defense (2011).

[791] M. Dempsey, interview by M. Zenko, 16 October 2012.

capacity to dictate strategic outcomes', especially in the context of great power competition[792]. Therefore, the key question for US air power is how it can, with futures being inherently uncertain, achieve the AFFOC's intent of delivering vigilance, reach, and power on a global scale?

Responding to this question in 2021 Lloyd Austin, US Secretary of Defense, confirmed that, in his view, the 2018 NDS did not provide sufficient air capability to meet the threat. Referring to the 'continued erosion of US military advantage vis-à-vis China and Russia in key strategic areas', he argued that future NDSs must either redress the balance or accept that a defeat at the hands of the PRC or Russia would in time be a fait accompli[793].

Examining these concerns, exploring the realities of the AFFOCs ambitions, and considering what a future NDS might need to offer US air power, the Mitchell Institute condenses the issue into three key points. Firstly, the 2018 NDS, despite its recognition of the QDR limitations, configured US air power to fight a single conflict. Failing to regain the Cold War emphasis on 'two-MRCs', it created a credible risk of failure during great power conflict, especially in the event of a second opportunistic aggressor[794].

Secondly, the Marshall Institute identifies that the 2018 NDS has not directed the US military to prepare for an extended-duration conflict[795]. Enhanced by the fact that such conflicts are likely to require the US, when compared to likely adversaries, to sustain operations at greater distance, a picture emerges in which it will have insufficient sustainable air power to operate against peer adversaries in their near abroad[796]. In such circumstances, any initial failure to deter or

[792] Cohen, "The Future of Warfare in 2030", 3.

[793] For Austin's comments, see:
L.J. Austin, "Senate Armed Services Committee Advance Policy Questions for Lloyd J. Austin Nominee for Appointment to Be Secretary of Defense", ed. US Senate (2021).
For the NDS, see:
US, "National Defence Strategy of the United States of America ".
For commentary, see:
M. Gunzinger, "Building the Future Force", *Air Force Magazine,* (2021).

[794] M. Autenrief Gunzinger, L. , "Building a Force That Wins: Recommendations for the 2022 Nationl Defense Strategy ", (The Mitchell Institute for Aerospace Studies 2021), 22-30.

[795] Ibid., 10-21.

[796] For US issues of operating air power at distance over prolonged periods, see:
J.A. Tirpak, "Next National Defense Strategy Should Return to Two-War Force Construct", *Air Force Magazine* 15 June 2021.

respond will ultimately lead to a long-term failure to contain or defeat likely near-peer threats.

Thirdly, the Marshall Institute concludes that a lack of 'all-domain warfighting concepts' undermines the value of any individual domain, including air. This ultimately creates a capability limited in its capacity to operate in modern warfare[797]. Though according to the US Pentagon this issue will be addressed by a Joint Warfighting Concept delivering Joint All-Domain Command and Control (JADC2), concerns over all-domain viability continue[798]. Of note, General John Hyten, Chairman of the US Joint Chiefs of Staff, commented in 2021 that adversary red teams had 'run rings' around US teams attempting to employ joint concepts[799]. Indicating that the US is unlikely to deliver air power supported effectively by all domains, one can conclude that this shortcoming will act to enhance, not resolve, the Marshall Institute's first two issues[800].

The air platform which has been widely predicted to resolve these three concerns is the F-35. Delivered through a multi-service, multi-national program within which the US was originally expected to acquire 2,456 aircraft, it became the largest acquisition program in US defence history[801]. However, the cost of the F-35 programme, which currently stands at $1.27 trillion, has despite bipartisan political support tempered purchasing aspirations and even led some to question the viability of the entire programme[802].

These financial concerns are further enhanced by long-running worries over whether the platform can be the multi-role air power panacea the US had expected. An example of this is issues with the F-35s 'Block 4' software upgrade

[797] Gunzinger, "Building a Force That Wins: Recommendations for the 2022 Nationl Defense Strategy ", 31-43.

[798] For an overview of the Joint Warfighting Concept and JADC2, see:
T. Hitchens, "New Joint Warfighting Plan Will Help Define 'Top Priority' Jadc2: Hyten", *Breaking Defense* 29 January 2021.

[799] J. Hyten, "Joint Cheifs of Staff Vice Chair on Defence Technology ", *Emerging Technology Institute* 26 July 2021.

[800] For further discussion on these challenges, see:
C. Dougherty, "Confronting Chaos: A New Concept for Information Advantage ", *War on the Rocks,* (2021).

[801] US, "Defense Primer: United States Airpower", ed. Congressional Research Service (2021).

[802] For figures on US F-35 procurement, see:
"F-35 Sustainment: Enhanced Attention to and Oversight of F-35 Affordability Are Neede", ed. US Government Accountability Office (2021).
For bipartisan political support for the F-35 programme, see:
J.B. Larson, Letter 17 March 2020.

which was expected to unlock the platforms full combat abilities through a complete weapons suite spanning both conventional and nuclear capabilities[803]. However, US Government reports in 2022 indicated that not only will Block 4 not be available to all F-35s but, forced by a timetable of 6-monthly updates, it and similar software developments continue to be 'immature, deficient, and insufficiently tested' before operational deployment[804].

When issues from cost to software are accounted for, questions develop as to whether the F-35 is the right answer for the US to meet the future great power competition. Firstly, US combat air power has become significantly smaller since the 1990s shrinking from approximately 4,000 combat aircraft in 1991 to just over 2,000 today. With the number of F-35s likely to drop from the original aspiration of 2,456, continued focus on the platform will further exacerbate this loss of combat mass. Secondly, with F-35s not being purchased as quickly as expected, the US air power fleet has begun to age from an average age of 8 years in 1991 to 27 years in 2022. With the likely adversaries concurrently increasing and modernising their air combat capabilities, the US is in the most contested areas of the world no longer guaranteed air superiority[805].

In addressing these challenges, General Brown asserted in 2021 that large numbers of exquisite, high technology but unreliable fighters could no longer be the answer for US air power. Rather, he argued for affordable, lightweight 'fifth-generation minus' platforms to replace the Cold War fleet of F-16s and compliment a much smaller than anticipated fifth-generation fleet[806]. Exploring how this strategic shift could be delivered, reports indicate that as a stop gap that may last into the late 2030s the US is elongating the service of older platforms. This includes the USAF's F-16s and F-15s and the USN's F-18s through structural and capability enhancements[807]. By doing so Deptula concludes that

[803] US, "F-35 Joint Strike Fighter (Jsf) Program", ed. US Congressional Research Service (2022).
[804] For non-availability of updates to all F-35s, see:
Ibid.
For the quote on the immaturity of software, see:
US, "F-35 Joint Strike Fighter (Jsf) ", ed. Office of the Secretary of Defense (2022).
[805] M. Kelley, "The Imperative to Field a Cutting-Edge Air Force", *Defense News*, 26 July 2021.
[806] C.Q. Brown, interview by D. Axe, 23 February, 2021.
[807] For background to the F-16 and F-15, see:
Staff Writer, "F-16 Fighting Falcon Multirole Fighter", *Air Force Technology*, 13 October 2021.

such fourth-generation aircraft may for the medium term deliver the bulk of US air operations. However, because of their comparative lack of sophistication they will be limited to 'relatively permissive air space'[808].

In examining this reality, the future of US air power appears to be moving towards a mass ability to operate in permissive air space. However, aligned to this, it must also operate its advanced but less reliable F-35s and F-22s in both limited numbers and highly contested air space against near-peer competitors. The question for the US is therefore whether in this era of great power competition it can successfully maintain an exceptional superpower role with a compromised air power capability. Furthermore, and in the context of this thesis, a central issue that must be addressed is whether the cyber vulnerabilities of this compromised capability might in themselves make US air power, and by extension its identity and role, untenable even before platforms take flight.

Cyber Vulnerabilities of US Air Power

In exploring the cyber vulnerabilities of US air power, an analysis of the topic offers a breadth of concerns which individually and collectively form a credible element to the broader cyber risk. Considering first cyber vulnerabilities which

For programmes being used by the US to extend the life of the F-16, see:
M. Garbarino, "F-16 Service Life Extension Program a 'Great Deal' for Department of Defense, Taxpayers", ed. United States Air Force Materiel Command (2018).
For reporting on the purchase of new F-16 and F-18, see:
S. Trimble, "U.S. Air Force Talks New F-16 Orders in Latest Acquisition Shake-Up", *Aviation Week*, 21 January 2021.
S. D'Urso, "The U.S. Air Force Is Considering Buying New F-16 Aircraft", *The Aviationist* 1 February 2021.
E. Tegler, "U.S. Navy Just Got Its First New F/a-18 Super Hornets — Here Are the Key Upgrade", *Forbes* 22 June 2020.
For detail on the F-15EX and considerations for new orders of the aircraft, see:
Boeing, "F-15ex: More Capabiity. More Capacity. More Savings. ", (2022).
M. Benitez, "F-15ex: The Strategic Blind Spot in the Air Force's Fighter Debate ", *War on the Rocks* (2019).
For Deptula's comments, see:
Deptula. D.A., interview by J.A. Tirpak, 1 October, 2019.

[808] For arguments why fourth-generation fighters retain utility, see:
"Keeping 4th-Gen Fighters in the Game."
K. Osborn, "Why the F-15 Eagle and F/a-18 Super Hornet Are Still Useful", *The National Interest,* (2022). B. Orgeron, "F-15ex and F-35a: The Future of American Air Superiority", *War on the Rocks* (2019).
For arguments on why fourth-generation aircraft are unviable in peer-on-peer operations, see:
Osborn, "Why the F-15 Eagle and F/a-18 Super Hornet Are Still Useful".
"Even with Upgrades, Chinese J-15 Are No Match for American Fighters", *The National Interest,* (2021).
For depth on the Next Generation Air Dominance (NGAD) program, see:
Staff Writer, "Ngad: Usaf's Sixth Generation Fighter Is on Schedule, Aquisitions Officals Say", *Aero Space Manufacturing* 11 October 2021.
J. Harper, "Air Force's Ngad Program 'Progressing Per Plan'", *National Defense* 21 September 2021.

could directly affect US air power, a prominent example that illustrates the depth of the issue is the F-35.

One of the world's most advanced combat aircraft, the F-35 continues to be procured by a growing number of Western states. Most prominently illustrated by Germany's 2022 announcement that it will invest $4.4 billion in the purchase of 35 F-35s, one might expect any identified cyber vulnerabilities to have been mitigated to a point at which they no longer pose a serious concern[809]. With the F-35 also expected to become the key air capability in any contested near-peer environment, this assumption is increasingly central to the viability of US air power.

Supporting this, the prime contractor, Lockheed-Martin, argues that the F-35 is the most lethal and survivable fighter aircraft in the world[810]. Achieved through the harnessing of digital technologies, it has created to some a 'new paradigm of air warfare' in which networked technologies enhance every element of air combat[811]. Though unquestionably advantageous in modern operations, the level of reliance created on these digital systems may be an 'Achilles heel' for the F-35. Considered in this context, the potential of cyber vulnerabilities that could be directly compromised by a hostile actor emerge as a significant consideration underlying the US's intent to maintain its exceptional superpower role.

Exploring these potential cyber vulnerabilities in more depth, the fundamental concern for modern interconnected systems is founded in data sharing across multiple networks. Though offering operational advantage, the process means that if a hostile actor finds a single vulnerability in any one node or point of entry, they can capitalise on the interconnections to introduce malware across all networks. In the case of air power, this can mean a single incursion resulting in the grounding of an entire fleet[812]. For the US who have already acknowledged that the bulk of their fourth-generation air power is not viable

[809] For the German purchase of the F-35, see:
P. Hille, "F-35: Why Germany Is Opting for the Us-Made Stealth Fighter Jet", *DW,* (2022).
[810] Lockheed-Martin, "The Most Advanced Fighter Jet in the World ".
[811] S. Roblin, "Who Deserves the Blame for the F-35's Many Computer Problems", *National Interest,* (2020).
[812] K. Osborn, "The F-35's Cyber Reliance Makes It Powerful—but Also Vulnerable to Attack", ibid. (2021).

against near-peer competitors, this risk becomes in relative terms deeply concerning.

Given this, the question is whether the US can guarantee, in the event of great power competition leading to near-peer conflict, those cyber vulnerabilities associated with its keystone air power asset can be effectively mitigated. In response, a key point of discussion is not necessarily the aircraft itself, but the supporting ground support systems. Referring in the F-35 case to ALIS and its replacement ODIN, both provide 'a comprehensive logistic support environment' which enables flight[813]. Integrating the F-35 'from tip to tail', these systems not only connect to the aircraft but are also networked back to Lockheed-Martin and, through Lockheed-Martin, to every other F-35 operator[814]. With Israel the only nation to have negotiated permission to amend or develop Lockheed-Martin's software, the reality is that despite sovereign data-diodes that should protect national elements of the programme, there remains a logical pathway from every global F-35 node back to the US fleet[815]. Therefore, any cyber vulnerability on ALIS or ODIN node anywhere in the F-35 programme could plausibly cause the loss of this keystone US air power capability.

Given the importance of this issue, one might expect the US to have ensured every possible vulnerability is identified and mitigated. However, the reality is that extensive issues have for some time been known of at the highest levels. For example, addressing the USAF Air Warfare Symposium in 2019 Heather Wilson, USAF Secretary, described ALIS as 'a proprietary system so frustrating to use that [its] maintainers are wasting 10-15 hours a week fighting with it…and looking for ways to bypass it to try to make the F-35 mission-capable'[816]. Although Wilson turned this into a joke suggesting that 'no Air Force maintainer will ever name their daughter 'Alice'', the issue is no laughing matter. Specifically, every time a frontline maintainer attempts such a bypass, they add additional cyber

[813] Henley et al., "Autonomic Logistics - the Support Concept for the 21st Century'", 417.
[814] Brissett, "Alis 2.02 Ready to Go".
[815] For detail on the Israeli version of the F-35, the F-35I Adir, see:
S. Roblin, "Israel's F-35 Stealth Fighters Can Strike Iran at Any Moment", *National Interest,* (2019).
For depth on the interconnectedness of ALIS and ODIN, see:
"Who Deserves the Blame for the F-35's Many Computer Problems".
[816] H. Wilson, interview by V. Insinna, 8 March 2019, 2019.

vulnerabilities to an already compromised system[817]. The result will, in the face of determined hostile actors, be the compromise of ALIS, the introduction of malware and the potential loss of the strategically vital F-35.

Wilson's concerns are underpinned by a series of public examples of vulnerabilities associated with ALIS. These range from USN penetration testers in 2012 exploiting Lockheed-Martin's failure to separate classified and unclassified data streams, through to USMC technicians in 2015 burning data to CDs and using commercial internet connections to transfer mission essential data[818]. When overlaid with recent reporting that the F-35 Block 4 software upgrade follows a longstanding programme trend of being 'immature, deficient, and insufficiently tested' before operational deployment, it can be concluded that cyber vulnerabilities undoubtedly exist within both the ground support system and the aircraft itself[819].

Based on these conclusions, the US should be justifiably concerned that in the event of great power competition leading to near-peer conflict, its fifth-generation air power will continue to exhibit exploitable cyber vulnerabilities. If successfully targeted by adversaries, these could not only lead to the disruption or removal from operations of the F-35 but, due to the platform's growing importance to the US, the loss of broader strategic advantage. At this point, the US would, through cyber vulnerabilities, be in danger of undermining its exceptional superpower role.

Looking further than cyber vulnerabilities directly connected to US air power, a second area of concern exists within the left-of-launch concept. Originating from the US's response to the 1991 Gulf War and an acceptance that its defences had

[817] Ibid.
[818] For detail on the USN penetration test example, see:
Shalal-Esa, "Lockheed's F-35 Logistics System Revolutionary but Risky".
For detail on the USMC example, see:
Grazier and Smithburger, "Pentagon Testing Office Calls Foul on F-35 Operational Testing".
US, "Observations on the Marine Corps F-35b Demonstration on Uss Wasp: Memorandum for under Secretary of Defense for Acquisition, Technology and Logistics", 1.
[819] For non-availability of updates to all F-35, see:
"F-35 Joint Strike Fighter (Jsf) Program".
For the quote on the immaturity of software, see:
"F-35 Joint Strike Fighter (Jsf) ".

failed to protect Israel from missile attacks, the left-of-launch idea emerged to prevent threats from ever taking flight[820]. Later driven forward by fears that 'rogue nations' including North Korea and Iran could soon field missile technologies able to threaten the US mainland, a 'full spectrum' missile defence programme that augmented conventional interception capabilities was implemented[821]. Focusing on non-kinetic means, this programme would in 2014 not only be acknowledged by the US Government but its cyber centric delivery confirmed[822]. Like all effective approaches to achieving strategic advantage, exploiting its adversaries' cyber vulnerabilities in the left-of-launch space would soon be redirected back at the US.

Amongst the potential left-of-launch vulnerabilities that the US should arguably be most concerned about is the air power supply chain. The means through which the US sabotaged North Korean missile launches in 2012, the approach follows the logic that the most easily accessible cyber vulnerabilities are likely to be found in less well protected civilian contractors rather than systems under military control[823]. Considered in terms of US air power, this logic was shown to be true through a 2018 CISA TA. In this, the CISA warned that Russian state actors had identified and exploited cyber vulnerabilities in, amongst others, US aviation supply chains[824].

Exploring the possible impact of such vulnerabilities, Oakley offers a series of potentially devastating scenarios for US air power[825]. Taking the introduction of logic bombs as an example, he argues that if an adversary were to identify and compromise US air power via the supply chain impacts may range from an operationally damaging loss of communications to catastrophic events such as

[820] Kemp, "Left of Launch: Countering Theatre Ballistic Missiles".

[821] For a discussion of the 'full spectrum' approach to missile defence, see:
Futter, "The Dangers of Using Cyber Attacks to Counter Nuclear Threats".
For an overview of the PAC-3 as an example of 'right-of-launch' means, see:
Staff-Writer, "Patriot Missile Long-Range Air-Defence System".

[822] US, "Missile Defence Review (2019)", IX.

[823] For depth on the North Korean example, see:
Lewis and Unal, "Cyberattacks on Missile Systems".

[824] US, "Alert (Ta18-074a) - Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, 15 March (2018)".

[825] Oakley, *Waging Cyber War: Technical Challenges and Operational Constraints*, 90.

platforms falling out of the sky[826]. With a 2010 compromise of US military hard drives supplied by technology company Seagate proving that such vulnerabilities exist and have been compromised, the US must now be concerned that its left-of-launch innovation may soon be the avenue through which it loses strategic advantage[827].

A second equally concerning set of left-of-launch cyber vulnerabilities for US air power are found in space-based assets. Growing in importance alongside air power's increasing reliance on space to support everything from communications, through navigation to kinetic strikes, the loss or compromise of US space-based assets via cyber vulnerabilities could materially impact its ability to operate[828]. Given this, the US must hope that the level of cyber assurance offered to all its essential space services would prevent the existence of exploitable vulnerabilities.

Considering this issue, Harrison et al note that though cyber attacks on space operations demand a high degree of sophistication, they do not require significant resources[829]. With options for such attacks ranging from the compromise of digital uplinks, downlinks, and crosslinks to the targeting of on-board space-based systems, a picture emerges of a breadth of opportunities for vulnerabilities to emerge[830].

Examining the likelihood of such theory progressing into fact, it was confirmed as early as 2007 that hostile actors linked to the PRC had already identified and exploited cyber vulnerabilities in the US Geological Survey's Lundsat satellite. In doing so, the PRC were able to cause twelve minutes of communications interference[831]. On a further occasion in 2014, hostile PRC linked actors again

[826] A Logic bomb is a form of malware that remains dormant until a specific condition is met. For depth, see:
Saeed, Selmat, and Abuagoub, "A Survey on Malware and Malware Detection Systems".
Agrawal et al., "Detecting Hidden Logic Bombs in Critical Infrastructure Software", 3.

[827] Menn, "Russian Researchers Expose Breakthrough Us Spying Program".

[828] For a discussion of air powers reliance on space, see:
EMEA, "Aviation: Satellite Services".
For comment on kinetic strikes reliance on space, see:
Perju, "Precision Guided Bombs: Analysis", 112.

[829] Harrison, Johnson, and Roberts, "Space Threat Assessment 2018", 4.

[830] Chen, "Opening Statement of Mr David D. Chen Independent Analyst: Hearing before the Us China Economic and Security Review", 75.

[831] Harrison, Johnson, and Roberts, "Space Threat Assessment 2018", 13.

compromised a US satellite. This time identifying cyber vulnerabilities in a commercial satellite station in Norway, the attackers managed to compromise the NASA Terra Earth observation satellites digital uplink. Having done so, reports indicated that despite not enacting the opportunity, all the steps necessary to take command of the satellite were achieved[832].

With further examples including a second PRC linked cyber attack on a US NOAA satellite adding depth, a picture emerges in which US space-based assets have exploitable cyber vulnerabilities[833]. If targeted by a hostile actor at a strategically imperative moment these could delay, disrupt, or even prevent air operations which rely on their output. Given this scenario, the US is presented with further evidence that left-of-launch cyber vulnerabilities could materially undermine its' air power and therefore strategic advantage.

A final but arguably most concerning area of US air power cyber vulnerabilities are the routes through which cyber espionage achieves its intent. Within this, the case study of the PRC targeting US air power technologies offers insight.

Seeking to overturn US superpower dominance, the PRC has actively pursued strategic advantage through military modernisation. In air power terms this has included the People's Liberation Army Air Force (PLAAF) and People's Liberation Army Navy (PLAN) developing not only the largest regional air power capability but one that in technological terms is competing with the world's most advanced states[834]. Illustrated in both the emergence of the PRC J-20 fifth-generation aircraft and its pursuance of sixth-generation technologies, this rebalancing of the strategic scales led Frank Kendall, US Secretary of the Air Force, to warn that the PRC is coming close to effectively countering US air power[835].

[832] Chen, "Opening Statement of Mr David D. Chen Independent Analyst: Hearing before the Us China Economic and Security Review", 75.

[833] US, "Us China Economic and Security Review Commission: 2015 Report to Congress", 296.

[834] For depth on PLAAF and PLAN aviation, see:

"Military and Security Developments Involving the People's Republic of China - Annual Report to Congress", ed. Department of Defence (2021), VI.

For a discussion of the development and capabilities of the H-6N, see:

R. Joe, "How the Descendants of a 1950s Bomber Transformed China's Strike Reach", *The Diplomat,* (2020).

[835] For reporting on a possible PRC carrier borne fifth-generation fighter, see:

R. Farley, "Is China Rethinking the Shenyang J-31 Fighter?", ibid., 13 November 2018.

Though domestic PRC ingenuity aligned with impressive technology and manufacturing industries cannot be ignored, an area that is viewed as central to this meteoric rise is the exploitation of US cyber vulnerabilities through espionage. In exploring this, one might expect the topic to be hidden from view with the US unlikely to publicly acknowledge such vulnerabilities. However, with commentators noting significant similarities between platforms such as the J-20 and F-35, it is unsurprising that evidence of such US vulnerabilities has emerged in the public domain.

One of the earliest such reports emerged through the 2015 Snowdon leaks. First confirmed by German newspaper *Der Spiegel,* it was alleged that PRC cyber actors had in 2007 exploited vulnerabilities in Lockheed-Martin systems to gain access to sensitive information on the F-35[836]. Whilst the Snowdon reporting does not confirm how the attack succeeded, what is evident is that through the information they obtained the PRC significantly closed the air power technology gap with the US.

Linking back to the above left-of-launch discussion on supply chains, it becomes evident how the exploitation of cyber vulnerabilities within a US civilian industry which holds on its systems the 'crown jewels' of US military technological advantage must be of particular concern[837]. Given this fact, it is of no surprise that such vulnerabilities have been the subject of not only extensive academic research but also official US attempts to manage them through formal mitigations such as CSCRM[838]. Notwithstanding such activity, US linked cyber vulnerabilities exploitable by persistent attackers continue to grow.

For discussion on the speed at which PRC air power has developed and future sixth-generation advances, see:
R. Joe, "Beyond China's J-20 Stealth Fighter", ibid. (2019).
For Kendall's comments, see:
F. Kendall, "State of Forces" (paper presented at the Air and Space Conference, 2021).

[836] Applebaum, "Nsa Preps America for Future Battle".

[837] Staff Writer, "Military Aircraft Market", (Fortune Business Insights, 2021).

[838] For a summary of academic research in this area, see:
K. Cheung, "Cybersecurity in Logistics and Supply Chain Management: An Overview and Future Research Directions", *Institute of Transport and Logistics Studies,* 146 (2021).
For recent US official direction to industry on countering the vulnerability, see:
J. Boynes, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations", ed. National Institute of Stnadards and Technology (NIST) (2021).

Looking back to 2011 to illustrate this, a major example of such a civilian cyber vulnerability exploited by the PRC was the compromise of the RSA SecureID system. A public-key encryption technology used to protect network resources in both industry and the public sector, SecureID is built around two factor authentication and the mathematical difficulty of factoring large numbers. In combining these, SecureID creates a robust means of stopping brute force attacks making it a standard encryption method for governments and large companies[839]. Given this apparent level of assurance, 2,838 organisations including major US aerospace defence contractors and US Government Departments are believed to use SecureID[840].

Despite this investment in SecureID, the product's integrity was undermined in 2011 by a hostile actor associated with the PRC. In this attack the key cyber vulnerability was not purely technical, but initially people based. Specifically, employees of RSA received an e-mail entitled '2011 Recruitment Plan'. Whilst directed to the system's junk mail folder, the e-mail was written convincingly enough to make employees believe it was genuine. Leading several of the emails and attached spreadsheets to be opened, the action led to a zero-day exploit being installed via a backdoor Adobe Flash vulnerability. Allowing the infiltration of Poison Ivy2 malware on to target devices the attackers next secured remote access allowing them to compromise further machines in the RSA network[841].

Having, through this process, gained access to strategic user accounts, the attacker exfiltrated secret SecureID keys known as 'seeds'. Once compromised, these 'seeds' allowed the attacker to theoretically clone the SecureID tokens which form one half of the two-factor authorisation. If paired with a password or pin number gained through other social engineering vulnerabilities, the PRC could have gained unfettered access to a target organisations sensitive system[842].

[839] Staff Writer, "What Is Rsa Securid?", (Barracuda, 2021).
[840] "Companies Using Emc Rsa Securid", (Enlytf 2022).
[841] Poison Ivy malware is a Remote Access Trojan (RAT) that was first identified in 2005. For depth, see:
US, "Poison Ivy ", ed. State of New Jersey (NJCCIC Threat Profile2017).
[842] For depth on the SecureID attack, see:
K. Krombholz, "Advanced Social Engineering Attacks", *Journal of Information Security and Applications,* (2014): 8.
A. Greenberg, "The Full Story of the Stunning Rsa Hack Can Finally Be Told", *Wired*, May 2021.

Labelled the 'the worst-ever hack of a cybersecurity firm to date', it acted as a pre-curser to the 2015 Snowdon revelations that US cyber vulnerabilities were leaving US air power open to compromise[843]. Though RSA would limit damage by quickly replacing the underlying certificates, the example was identified in 2012 by General Keith Alexander, Commander of the US Cyber Command (CYBERCOM), as having far reaching consequences. Explaining the breach in testimony to the Senate Armed Services Committee, Alexander commented that if a highly respected cyber security company such as RSA could be compromised, then virtually any company holding sensitive US military information is vulnerable. In such circumstances, any military technological advantage the US may hold over adversaries including the PRC is likely to be lost[844].

With Alexander repeating his warnings on espionage to the US Congress in 2014, it is evident that supply chain cyber vulnerabilities undermining US strategic advantage through espionage are unlikely to abate[845]. With the above example of PRC air power illustrating how exploitation of such vulnerabilities has acted to shift the Asia-Pacific balance of power, the strategic impact of US cyber espionage vulnerabilities is confirmed[846]. Persisting into the 2020s with the NSA commenting that cyber espionage continues to shift the strategic Sino-Western balance of power, the conclusion is clear: the exploitation of cyber vulnerabilities through espionage has in the long term the potential to be the most impactful element of US air power cyber risk[847].

[843] "The Full Story of the Stunning Rsa Hack Can Finally Be Told".

[844] For Alexander's testimony to the US Senate, see:
Senate Armed Servies Committee, "Hearing to Recieve Testimony on Us Strategic Command and Us Cyber Command in Review of the Defense Request for Fiscal Year 2013 and the Future Years Defense Programe", ed. US Senate (2012).

[845] For Alexander's comments to the US Congress, see:
US, "Department of Defense Authorization for Appropriations for Fiscal Year 2013", ed. US Congress (2014).

[846] Gady, "New Snowdon Documents Reveal Chinese Behind F-35 Hack".

[847] US, "Cybersecurity Advisory - Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities ", ed. National Security Agency (NSA) (2020).

Conclusions on US Air Power Cyber Vulnerabilities

The above discussion chartered the development of the US towards an assumed role as a global superpower with the self-perceived right to export and enforce its version of liberal democracy. Maintaining a large military lever to achieve this, the US was still found to be falling short of the mass to achieve the unilateral multi-front activity required for this role. Though through this circumstance air power becomes a keystone force multiplier, the US capability was itself shown to be increasingly reliant on a reduced number of advanced air platforms. This has, it was concluded, undermined the ability of US air power to have the necessary impact.

Considering the cyber vulnerabilities to US air power in this context, it is identified how any digital compromise could further undermine the US ability to maintain its role. Delivered through discussions on direct, left-of-launch and espionage related vulnerabilities, such a compromise was shown to be a credible possibility. Reflecting on this, air power cyber vulnerabilities emerge as a potential 'Achilles heel' with strategic relevance which may impact the US's desire to protect its superpower role.

United Kingdom (UK): Residual Great Power

Introduction to UK Air Power's Cyber Vulnerabilities

Exploring the cyber vulnerabilities to UK air power, this section will initially chart the UK's gradual decline from superpower status to a residual great power struggling to maintain its global aspirations. Having offered an overview of the impact on the UK's diplomatic and economic levers of power, the discussion will focus on identifying how its military instrument has also been challenged. Choosing to replace mass with Science and Technology (S&T) advantage, this trend will be shown as continuing into air power with a likely future of a small number of manned F-35B aircraft supported by a larger Unmanned Combat Air Vehicle (UCAV) fleet.

Considering this balance with reference to cyber vulnerabilities, it will be noted that UK air power could, through the exploitation of identified vulnerabilities, lose a notable proportion of its air power. Taken collectively with the role to which the UK aspires, the section will ultimately conclude that UK air power's cyber vulnerabilities must not be viewed as a technical or military issue, but a national concern if the state is to remain a residual great power with global relevance.

The UK: From Superpower to Residual Great Power

Never hegemonic, the UK was for approximately four hundred years a superpower[848]. Emerging as such by the 16th century, it would into the 20th century maintain direct influence over a quarter of the globe[849]. A position forged through a realist desire to expand beyond geographically limited shores, the duration and scope of the Empire would have long-reaching impact. Morphing the national psyche into a constructivist explained role most succinctly described as 'Global Britain', its legacy is of a nation not only believing in an ability, but also a duty, to exercise global reach and influence[850].

Despite being deeply entrenched, this 'Global Britain' role would from the post-war period be increasingly challenged. As national movements of self-determination alongside social and fiscal effects of the Second World War took hold, the Empire all but disappeared[851]. Losing most of its Colonies by the 1960s, the impact was illustrated in the 1956 Suez Canal Crisis when an old-Colonial

[848] Buzan, *Regions and Powers* 65.

[849] For depth on the history of the British Empire, see:
T. Lloyd, *Empire: A History of the British Empire* (London: Hambledon, 2001).

[850] It is acknowledged that the phrase 'Global Britain' has gained political popularity since its use by Prime Minister May in 2017 and more recently was adopted by Prime Minister Jonhson's Government as a refrain on the opportunities of Britain's exit from the European Union (BREXIT). However, as a term relating to Britain's self-endorsed role, it has providence since the 16th century.
T. May, "The Government's Negotiating Objectives for Existing the Eu: Pm Speech", ed. Cabinet Office (Gov.UK2017).
HMG, "Collection: Global Britain – Delivering on Our International Ambition ", (Gov.UK2017).

[851] For depth on the impact of the Second World War on the UK, see:
P. Addison, "The Impact of the Second World War," in *A Companion to Contemporary Britain: 1939-2000*, ed. P. and Jones Addison, H. (Oxford: Oxford University Press, 2005).
For depth on national self-determination, see:
F. Roosevelt, "Four Freedoms Speech, State of the Union Address", (Franklin D. Roosevelt Presidential Library 1941).
S. Pederson, *The Guardians: The League of Nations and the Crisis of Empire* (Oxford: Oxford University Press 2015).
A. Clayton, *The British Empire as a Superpower, 1919 - 39* (Georgia University of Georgia Press 1986).

alliance of France and the UK were forced to withdraw troops attempting to secure the canal under US and Russian pressure[852]. Proving that the UK was no longer a superpower with unilateral global reach, one might have expected 'Global Britain' to be diminished. Conversely, the UK continued to pursue its superpower inspired self-image throughout the Cold War in the guise of a great power with global reach.

Successfully achieved throughout the late 20th century, the tools at the UK's disposal were not insignificant. Of these, the most prominent was its permanent seat on the UNSC. Borne from meetings between the US, Soviet Union, and the UK in 1941 to 1945, the UNSC, and more broadly the UN, were products of how these states envisioned the post-war world order. Creating structures that placed unassailable global security influence into the hands of the UNSC permanent members[853], the UK, by securing one of these seats, retained global influence that would underpin its role[854].

Concurrent to the UNSC, this global intent was underpinned by what Winston Churchill summarised in 1948 as the '3 majestic circles' of the Commonwealth, a united Europe, and the English-speaking world[855]. Considering first the Commonwealth, the organisation was loosely established in the 1926 Balfour Declaration and formalised in the 1949 London Declaration[856]. Though later characterised by consensus politics, its origins are best explained through a UK

[852] For depth on the Suez Canal Crisis, see:

Calvocoressi, P. *World Politics Since 1945 P. Calvocoressi, World Politics since 1945 (London: Longman 1996), 377-84., 7th Ed* (1996) (London: Longman).

[853] These US structures would place power principally into the hands of the Permanent Members of the UNSC who would hold veto authority. These were the US, Russia (initially the Soviet Union), the UK, France, and the PRC. For depth on the UNSC, see:

D.L. Bosco, *Five to Rule Them All: The Un Security Council and the Making of the World* (Oxford: Oxfrod University Press 2009), 10-38.

United Nations, "1944-1945: Dumbarton Oaks and Yalta ", ed. UN Secretariat (2020).

[854] For a discussion on whether the UK as a declining power was justified in being a permanent member of the UNSC, see:

C. Wrigley, *Churchill* (London: Haus, 2006), 29.

[855] For Churchills '3 circles' characterisation, see:

W. Churchill, "Conservative Mass Meeting: A Speech at Llandudno," in *Europe Unite Speeches 1947 and 1948* ed. R.S. Churchill (London: Cassell, 1950).

For other similar metaphors used by politicians including Ernest Bevin and Anthony Eden's, see:

A. May, "The Commonwealth and Britain's Turn to Europe: 1945-83", *", The Round Table: The Commonwealth Journal of International Affairs,* 1, no. 102 (2013): 30.

A. Deighton, "Britain and the Three Interlocking Circles," in *Europe 1945-1990s: The End of an Era?*, ed. A. Varsori (London: MacMillan), 1990), 155.

[856] For depth on the 1929 and 1949 Declarations, see:

HMG, "Imperial Conference 1926 – Inter-Imperial Relations Committee: Report, Proceedings and Memoranda (the London Declaration)", ed. Commonwealth (London 1926).

desire to mitigate the loss of Empire by establishing a UK led 'third' global force to balance the Cold War poles of the US and Soviet Union[857]. Whilst it is debatable whether this was achieved, the fact of the Commonwealth's creation, and the willingness of newly independent states to become members and align themselves to UK leadership was telling. Specifically, it highlighted how it was not only the UK who believed itself to be a great power, but the international community that accepted it as such[858].

The second 'circle', European cooperation, was built on the conviction that Europe should never again submit to totalitarian terror and war. Notably driven by the UK through Churchill's post-war calls for a 'United States of Europe', its original 1949 form as the Council of Europe saw the UK assume a leading role[859]. Even when the UK became resistant to further European integration in the 1950s, a position epitomised by Churchill's 1953 statement of the UK being 'with them but not 'of' them', Europe's importance in underpinning the UK's global leadership was undiminished[860]. This was illustrated by the fact that even when pulling away from Europe, the UK was able to dictate its relationship with other European powers[861].

Finally considering the English-speaking world, a concept more accurately identified as Anglo-US relations, this emerged in the post-war period as the so-called 'special relationship'[862]. A term popularised by Churchill in 1946, its true

[857] K. Srinivasan, *The Rise, Decline and Future of the British Commonwealth* (Basingstoke: Palgrave MacMillan, 2005), 8.

[858] For a discussion of the development, strengths and limitations of the Commonwealth during the Cold War see:
S. Onslow, "The Commonwealth and the Cold War, Neutralisation and Non-Alignment", *The International History Review,* 37 (2015): 1065.

[859] For comments on the 'United States of Europe', see:
W. Churchill, "Tragedy of Europe Speech: Zurich, 19 September 1946", http://www.churchill-society-london.org.uk/astonish.html#:~:text=I9th%20September%201946.,about%20the%20tragedy%20of%20Europe.&text=If%20Europe%20were%20once%20united,hundred%20million%20people%20would%20enjoy.
For further depth on the origins of the Council of Europe, see:
Council of Europe, "Statute of the Council of Europe", (1949), 1.
D. Tarschys, "The Council of Europe: 50 Years of European Cooperation", *European Review,* 7, no. 5 (1999).

[860] For the quote, see:
W. Churchill, "House of Commons Debate, 11 May 1953 at 3.32pm – Foreign Affairs", ed. Hansard (1953).

[861] For depth on Britain's resistance to a federal Europe, see:
D. Gowland, Turner, A. , *Britain and European Integration 1945-1998: A Documentary History* (New York Routledge, 2010), 4.
S. Dockrill, *Britain's Retreat from East Suez: The Choice between Europe and the World* (Basingstoke: Palgrave MacMillan, 2002), 8-22.
For depth on Britain's resistance to seeding sovereignty to Europe, see:
S. Rosato, *Europe United: Power Politics and the Making of the European Community* (New York: Cornell University Press, 2011), 104-68.

[862] For depth on US-British relations, see:
R. Ovendale, *Anglo-American Relations in the Twentieth Century* (Basingstoke MacMillan, 1998).

meaning has been characterised as the 'device of a declining power trying to harness a rising power to serve its own ends'[863]. A more pragmatic explanation, however, highlights the value for both sides. Ranging from joint military operations to the UK as the US's gateway to Europe, it removes sentimentalised interpretations[864]. In doing so, it not only explains the relationship but also how since the Second World War the UK has extended its global reach by staying within the decision-making cycle of a superpower[865].

In reflecting on the UNSC and the 'three circles', alongside membership of other supranational organisations that have buoyed its influence, it is evident that despite the loss of Empire the UK retained a global great power role[866]. Notwithstanding this, the role has, in the 21st century, become less certain.

Considering this contemporary position, Blair and Curtis argue that following a period of relative decline the UK no longer has the depth to claim legitimate global influence and, therefore, a great power role[867]. Countering this, one could argue that the UK continues through key memberships of the UNSC and other supranational bodies to maintain its 20th century position. Though logical, such optimism ignores recent events that have diminished the 'three-circles' to a point at which global influence is legitimately questioned.

The first of these is Britain's Exit from the EU (BREXIT). With EU membership anchoring the UK as an 'influential actor on the world stage' for half a century, its departure has had impact[868]. Trying to put a positive spin on this, pro-BREXIT UK politicians argue that it represents an opportunity for a 'freed' UK to be

[863] The term 'special relationship' first emerged in 1917 but would be popularised by Churchill's 1946 'Iron Curtain' speech.

W. Churchill, "The Sinews of Peace (Iron Curtain Speech)", https://winstonchurchill.org/resources/speeches/1946-1963-elder-statesman/120-the-sinews-of-peace/.

For depth on the US-Anglo relationship and arguments on its use as a UK device to hold onto power, see:

D. Reynolds, "A 'Special Relationship'? America, Britain and the International Order since the Second World War", *International Affairs,* 62, no. 1 (1986): 2.

[864] W. Wallace, Phillips, C. , "Reassessing the Special Relationship", ibid.5, no. 2 (2009): 265.

[865] M. Beloff, "The Special Relationship: An Anglo-American Myth?: Essays for A.J.P. Taylor," in *A Century of Conflict: 1850-1950*, ed. M. Gilbert (London: Hamish Hamilton, 1966), 153.

[866] Examples of supranational organisations include the North Atlantic Treaty Organisation (NATO) and the Group of Eight (G8). For depth on these, see:

P.I. Hajnal, *The G8 System and the G20 Evolution, Role and Documentation* (London: Routledge, 2019), 14.
NATO, "Member Countries", (2020).

[867] A. Blair, Curtis, S. , *International Politics: An Introductory Guide* (Edinburgh Edinburgh University Press, 2009), 47.

[868] K. Oppermann, Beasley, R., Kaarbo, J. , "British Foreign Policy after Brexit: Losing Europe and Finding a Role", *International Relations,* July (2019): 5.

'great'[869]. However, Oppermann et al argue that the UK's post-BREXIT future is likely to be either as a 'faithful ally to the US' or an 'isolate'[870]. In either circumstance, Hill concludes, the UK will find itself pushed to the margins of diplomatic discussion in 'an exposed and chilly experience' that is not reflective of a great power[871].

Beyond Europe, the Anglo-US 'special relationship' has also become 'not so special'[872]. Whilst this centres on the assertion that following BREXIT Britain no longer offers the US valuable access to Europe, it was stoked by differences between Johnson and Biden[873]. A division which began with Johnson advocating for BREXIT against the advice of the Obama-Biden Administration[874], the distance increased through ill-advised comments by Johnson regarding both Hillary Clinton and President Obama[875]. Finally cemented by Johnson's courtship of the Trump Administration[876], the picture is of a Biden Administration disinclined to help Britain overcome the impact of BREXIT.

In contrast, it is acknowledged that this downturn in the 'special relationship' has been countered by public shows of friendship[877] and Defence cooperation

[869] For examples of speeches and statements made by UK politicians on the theme of global diplomatic promise post-BREXIT, see:

B. Johnson, "Foreign Secretary Announces 250 New Diplomatic Roles and Ten New Sovereign Missions", ed. Gov.UK (Gov.UK2018).
T. May, "Pm Speech at Munich Security Conference", ed. Cabinet Office (Gov.UK2018).
J. Hunt, "Foreign Secretary Hunt: Britain's Role in a Post-Brexit World", ed. FCO (Gov.UK2019).
D. Raab, "Global Britain Is Leading the World as a Force for Good", *The Telegraph* 21 September 2019.

[870] "Global Britain Is Leading the World as a Force for Good".

[871] C. Hill, "What Next for British Foreign Policy in a Post-Brexit World?", *The Guardian*, 18 August 2019.

[872] R. Heath, "Britain Braces for Not-So-Special Relationship with Biden", *Politico* 31 December 2020.

[873] This claim has been notably made by former senior UK Diplomat Peter Ricketts who stated that 'when Biden looks towards Europe, he will see Paris and Berlin as the centre of gravity…and Britain will be seen as an outlier'.

P. Ricketts, interview by C. Gallardo, 26 October 2020.

[874] For example, in an April 2016 press-conference Obama warned that if Britain left the EU it would be at the 'back of the queue' for a trade deal with the US.

B. Obama, interview by K. Calamur, 22 April 2016.

[875] For detail on Johnson's comments, see:

B. Johnson, interview by R. Sanchez, 10 February 2015.
"Uk and America Can Better Friends Than Even Mr Obama…If We Leave the Eu", *The Sun* 22 April 2016.

[876] Commenting on this courtship after a joint press conference in New York in September 2019 in a period when both Trump and Johnson were facing domestic troubles, the media characterised their relationship as close. Of note, the New York Times skited 'if nothing else, they have each other'.

P. Baker, "Trump and Johnson, Together on the World Stage, Eye Troubles Back Home", *The New York Times*, 24 September 2019.

[877] An example of public shows of friendship but a private retention of distrust from the US is offered in the September 2021 meeting held as a sidebar to the 2021 UN General Assembly. For depth and analysis, see:

US, "Readout of President Joseph R. Biden Jr.'S Meeting with Prime Minister Boris Johnson of the United Kingdom", ed. The White House (2021).
E. and Toosi Casalicchio, N. , "Joe Biden Keeps Boris Johnson Guessing", *Politico* 21 September 2021.

including AUKUS[878]. It is also noted that following the election of Prime Minister Sunak, some commentators have suggested that shared ambitions from countering Russia to addressing the climate crisis may offer 'an opportunity to turn the page on an awkward time in transatlantic relations'[879]. However, notwithstanding this optimism, it remains evident that a shifted reality endures in which the US is likely to turn more readily to Germany than the UK for European focused engagement[880]. Given this, the UK's global reach will be more difficult to maintain without the unswerving assurances and support of its superpower ally.

Finally considering the Commonwealth, the organisation through its failure to respond to contemporary issues including its members antidemocratic tendencies and human rights violations has become considered by many as no longer globally relevant[881]. Whilst the roots of this decline may have emerged in the Cold War, it is increasingly clear that the Commonwealth lacks the meaningful depth to help maintain a 'Global Britain'.

Beyond this diminished diplomatic influence, the UK has also struggled to maintain the relative economic advantages of a once leading trading nation. Currently ranked as the world's fifth or sixth largest global economy depending on the model, Britain has on all scales declined since the Cold War[882]. Projecting to 2050, Price Waterhouse Cooper (PWC) further predict that though the UK will keep pace with traditional competitors, it will be outperformed by emerging

[878] For depth on AUKUS, see:
UK, "Uk, Us and Australia Launch New Security Partnership", ed. .Gov.UK (2021).
The Economist Briefing, "Aukus Reshapes the Strategic Landscape of the Indo-Pacific", *The Economist* 25 September 2021.

[879] For comment on the Anglo-US relationship following the election of Prime Minister Sunak, see:
US, "Readout of President Joe Biden's Meeting with Prime Minister Rishi Sunak of the United Kingdom", ed. The White House (2022).
D. Leal, "How Rishi Sunak Can Reset the Us-Uk Special Relationship", *The Hill*, 29 December 2022.

[880] For a history of the US-German relationship, see:
US, "Us Relations with Germany", ed. US DEpartment of State (2022).
For depth on recent developments in the US-Germany relationship, see:
D. Kochis, "Winds of Change in Berlin? A Road Map for U.S.–German Relations", *Heritage Foundation* (2021).

[881] The Week Online, "The Commonwealth: Why It Struggles to Remain Relevant", *The Week*, 1 August 2014.

[882] For example, the Centre for Economics and Business Research places the UK as the 5th largest global economy in 2020, falling from 4th in 2005 and predicted to fall further to 6th by 2025. However, the PWC published Global Economy Watch places Britain 6th in 2020.
"World Economic League Table, 2021: A World Economic League Table", (Centre for Economics and Business Research, 2020).
"Global Economy Watch: Prediction for 2021", (PWC, 2021).

economies such as Brazil, Indonesia, and India[883]. Resulting in a relative drop in its global economic position by 2050 to ninth, the economic outlook may not be disastrous but still signals a move away from its 19th century heyday[884].

Though this 2050 top ten position allows the UK to retain credible claims of being a global economic power, Morris identifies that to be considered a great power with global reach it must translate residual economic strength into projected influence[885]. In considering this, soft power offers a telling metric[886]. Though accepted as important by successive UK Governments [887], the Johnson Government decided in 2020 to merge the Department for International Development (DFID) with the Foreign and Commonwealth Office (FCO) creating the Foreign, Commonwealth and Development Office (FCDO). Citing economic pressures[888], the new organisation not only had to divide its resources but do so with a reduced spending commitment of 0.7 percent to 0.5 percent of GDP[889]. A decision criticised by opponents as fundamentally wrong, politically foolish and an act of national self-harm, it has been characterised as materially undermining UK global influence[890].

This trend of decline was further exacerbated by the COVID pandemic. Though more impactful for the UK than other comparable states[891], it has not caused

[883] J. Hawksworth, Clarry, R., Audino, H. , "The Long View: How Will the Global Economic Order Change by 2050?", (PWC, 2017).

[884] B. Elbaum, Lazonick, W., "The Decline of the British Economy: An Institutional Perspective", *The Journal of Economic History,* 44, no. 2 (1984): 570.

[885] J. Morris, "How Great Is Britain? Power, Responsibility and Britain's Future Global Role", *The British Journal of Politics and International Relations,* 13, no. 3 (2011): 333.

[886] Nye defines soft power as the art of 'getting others to want the outcomes that you want' through co-option rather coercion.
Nye, "Public Diplomacy and Soft Power", 95.

[887] For example, see Prime Minister Cameron's comments on 'combating poverty, disaster and conflict' in 2011.
D. Cameron, "Uk Aid: Changing Lives, Delivering Results", ed. Department for International Development (DFID) (2011), 4.

[888] For detail on the financial pressures which led to the creation of the FCDO, see:
A. Dickinson, "Spending Review: Reducing the 0.7% Aid Commitment", ed. House of Commons Library (2020).
For criticism of the decision to reduce aid spending in November 2020, see:
L. Snugg, interview by BBC News Online, 2020.
J. Welby, "Archbishop of Canterbury: Uk Must Keep Its Foreign Aid Promises", *Financial Times* 2020.
D. and Blair Cameron, T. , "Cutting Aid Budget Would Hit Uk Influence, Two Former Pms Say", *Reuters Online*, 21 November 2020.

[889] For depth on the spending reduction, see:
UK, "International Development Act", ed. HMG (2015).
"Spending Review: Reducing the 0.7% Aid Commitment", ed. House of Commons Library (2020).

[890] L. Suggs, interview by C. Gallardo, 25 November 2020.

[891] For depth on the disproportionate impact of COVID on the UK, see:
International Monetary Fund, "World Economic Outlook: The Great Lockdown", (2020), xiv.
D. David, "Coronovirus: Uk Worst Hit among Major Economies", *BBC News Online*, 26 August 2020.

seismic economic change. However, it has increased the pace of an existing downward trajectory. In doing so, the economic impact of COVID will bring the UK closer to a situation in which it struggles to generate the economic resources necessary to maintain a great power role.

Collectively, the degrading influences experienced in the early 21st century have shifted the UK's global position. Already unable to act unilaterally in the Cold War, the UK will find it increasingly hard to project diplomatic or economic influence on a global scale. Conversely, however, the UK is still in the top ten economies and retains membership of key transnational institutions. As such, its relative decline does not mean that it faces an existential threat or has even fallen out of the great power categorisation. Rather, by harnessing its remaining influence, the UK can be regarded as a residual great power able to maintain its realist-constructivist global aspirations forged in the age of Empire. However, in striving to do so it is operating against a backdrop of limitations defined by relative decline.

The UK's Military Instrument: Reducing Mass and a Reliance on Technology

It is evident that the UK has diplomatically and economically declined from its age of Empire to a 21st century residual-great power role. Though these levers are essential in understanding a nation's role, both are in the realist sense limited. Specifically, to have impact, the diplomatic and economic levers must be backed by persuasive military means. Coalescing around the contention that security, competition, and war make the military 'stick' essential for states to thrive and even survive, one must to understand the nature and credibility of the UK's residual great power role explore its military instrument[892].

Examining this issue from a positivist perspective, an economic measurement that offers this understanding is whether the UK is achieving the NATO defence spending target of 2 percent of GDP. Though to some an ambiguous yardstick

[892] For an expansion on this realist argument on the importance of the military instrument, see:
Mearsheimer J.J., *The Tragedy of Great Power Politics* (New York: Norton Publishing Company, 2001), 97.

intended to control post-Cold War spending reductions, the target has nonetheless become a measurable 'line in the sand' invoked by some NATO members, most notably the US, to hold others to account[893]. Therefore, if the UK's 21st century global aspirations have validity one can conclude that it must be achieving, if not exceeding, the target. This assumption was reinforced by the UK itself through its 2021 Integrated Review (IR) which recognised the target as integral to achieving a 'Global Britain'[894].

Analysis of UK Defence spending, however, shows gradual reduction from its 1960 height of over 6 percent of GDP to a sub-target low of 1.7 percent by 2018[895]. Though this trend was claimed as being reversed in 2021 when the UK's Spending Review (SR) announced a 4-year increase in the Defence budget by £24 billion, the situation is not as simple as the headlines suggest[896]. Explained by Dempsey, the UK Government's announcement added the cash difference between Financial Year (FY) 2020/21 and each subsequent year, ignoring the conventional method of taking the difference between years start and end[897]. If convention had been followed, the spending announcement should have only claimed a 4-year increase of £7bn.

This example of 'spinning' figures for political gain indicates that even though spending may have increased, there is no guarantee that the UK is meeting the 2 percent target. For example, Julian Lewis MP, Chairman of the British Parliamentary Defence Select Committee, explains that the UK Government has in recent years included previously unlisted elements such as UN Peacekeeping contributions and pensions within official figures. If it had not, Lewis concludes

[893] Speaking at the NATO summit in London in December 2019 President Trump stated that he would 'deal with… [the] delinquent' NATO states who were continuing to fail to spend 2 percent of their GDP on defence. These comments were made against the backdrop of the US in FY 2018/19 spending $732bn on Defence, equating to 3.4 percent of its GDP.
D. Trump, interview by A. Woodward, 3 December 2019, 2019.
Statistica, "The 15 Countries with the Highest Military Spending Worldwide in 2019"; A. Mesterhazy, "Burden Sharing: New Commitments in a New Era", ed. NATO Parliamentary Assembly Defence and Security Committee (2018).

[894] UK, "Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy", 100.

[895] World Bank, "Military Expenditure (% of Gpd) – United Kingdom ", (2019).
UK, "Finance and Economics Annual Statistical Bulletin: International Defence 2019 ".

[896] For SR, see:
"Spending Review 2020", ed. HM Treasury (2020).
For arguments that the SR mislead, see:
B. Zaranko, interview by J. Bealse, 19 November 2020.

[897] N. Dempsey, "Uk Defence Expenditure", ed. House of Commons Library (2021).

that 'on a like-for-like basis the UK would in 2019 have only spent 1.8 percent of GDP on Defence'[898]. This proves the opaqueness of UK Defence spending.

Reflecting on this, two judgements can be made. Firstly, the political spinning of defence spending illustrates the UK's enduring desire to present itself as a great power, albeit a residual great power, able to deliver global influence. Secondly, despite the intent, the UK's military lever shows the same declining trend as in the diplomatic and economic spheres. No longer able to offer clarity in its ability to meet the NATO target, the implications for the UK are likely to manifest in an inability to offer credible coercive force to support global aspirations. Though not coming near to an existential threat, this brings into question the UK's ability to thrive in the 'Global Britain' role.

Though appearing conclusive, a counterargument is offered by the UK Government through its focus on replacing mass with S&T advantage. Central to the IR, this is built around the intent to become a S&T 'superpower' by 2030 with the advances this brings harnessed as a key 'component of national security'[899]. Brought into military focus by the UK's Defence Command Plan (DCP) and the MOD S&T Strategy, the intent is to deliver technologically advanced battle-winning capabilities [900] . When fielded, these are heralded as 'game changing…[developments that will ensure] a global reach that sets the UK apart from other countries'[901].

Adding depth, the UK has concurrently reinvigorated its military doctrine through the Integrated Operating Concept (IOpC)[902]. Embedding S&T at its core, the IOpC outlines a 'new approach to the utility of armed force' in which technology replaces mass as the deciding factor of global relevance[903]. A theme continued throughout the IOpC's protect, engage, contain and warfighting phases, S&T

[898] Lewis, "Defence Spending Continues to Decline".
[899] UK, "Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy", 11.
[900] Ibid.
UK, "Science and Technology Strategy", ed. Ministry of Defence (2020).
[901] Great Britain. Ministry of Defence, *Defence in a Competitive Age,* March (2021): 11.
[902] UK, "Integrated Operating Concept (Iopc)", ed. Ministry of Defence (2021).
[903] ibid., 5.

advantage becomes a 'golden thread' to the military's support of the globally focused vision.

Intending to seize opportunities and pre-empt future threats through an 'integrated high-tech armed force'[904], this direction of travel is underpinned by Dame Angela McLean, the MOD's Chief Scientific Adviser (CSA), who asserted that S&T will achieve 'a decisive edge [for the UK] in future conflict'[905]. If accepted, one could conclude that this advanced UK military instrument will, despite reductions in funding and mass, balance relative decline to assure the global residual great power role.

Reflecting on this, the UK can be characterised as entering a period in which the military is balancing relative economic and diplomatic decline. By doing so using technological advantage to replace mass, it is effectively shoring up the constructivist residual great power role. However, what remains unanswered is whether these developments have introduced cyber vulnerabilities which may undermine the UK's growing reliance on digitised capabilities and, therefore, the achievement of this intent. To explore this, air power offers an ideal case study.

UK Air Power: Technological Advancement at a Cost

To consider the role air power plays in assuring the UK's residual-great power role, an intuitive focus is combat air. In this, other elements of air power from Air Transport (AT), through Air-to-Air Refuelling (AAR) and Intelligence, Surveillance, Targeting and Reconnaissance (ISTAR) are not dismissed as unimportant. However, it is a state's ability to project power through combat means that is not only decisive in a realist context, but also the clearest demonstration of a state's ability to assure its role. This is illustrated by examples including Western operations in Libya and those to counter ISIS in Iraq and Syria. In both, air power

[904] UK, "Science and Technology Strategy", 11.
[905] Ibid., 4.

was used above the deployment of ground troops to project power. This proved combat air as an essential component of contemporary statecraft[906].

The validity of this argument is acknowledged by the UK in its 2018 Future Air Combat Strategy. Stating that air power is critical to the UK's ability to 'deliver our national security and to support the Government's vision for a strong, prosperous, influential and global Britain', the capability is accepted as forming a major contribution to UK operational success [907] . With the strategy further acknowledging that 'the viability of combat air must be maintained if the UK wishes to remain a credible warfighting power', it is evident that combat air will form a central pillar to the state's current and future military instrument[908]. To achieve this, the UK intends to build its future capability around two elements: F-35 and the Tempest programme[909].

Beginning with F-35, the aircraft entered service with the RAF in 2018 as a fifth-generation multi-role capability expected to operate alongside the Typhoon[910]. Acquired by the UK in the form of the carrier borne Short Take-Off and Vertical Landing (STOVL) variant, the capability's combination of low observability (or 'stealth') and advanced technologies have seen it heralded as a strategic gamechanger and the 'best fighter in the world'[911]. Though impressive, Baroness Goldie, Minister of State for Defence, confirmed on 16 December 2020 that due to financial pressures the UK has reduced its initial order of 138 F-35s to a

[906] For further depth on the UK's role in Libya and against ISIS, see:
Mueller, *Precision and Purpose: Airpower in the Libyan Civil War*
Fishel and Stein, "Lessons Learned from the Air War against the Islamic State".

[907] UK, "Combat Air Strategy: An Ambitious Vision for the Future ", ed. Ministry of Defence (2018), 6.

[908] J. Bronk, "Combat Air Choices for the Uk Government", *RUSI,* (2020): v.

[909] For details of these cornerstones, see:
UK, "Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy".
"Combat Air Strategy: An Ambitious Vision for the Future ", 6.
It is noted that a 3rd cornerstone is the Typhoon. However, planned to leave service in 2030, this discussion will focus on the F-35 and the Tempest programme as the future intent of the UK. For future depth on the Typhoon and its planned departure from service, see:
Eurofighter Typhoon, "Our History", (2021).
G. Jennings, "Uk Defence Command Paper: Raf to Axe Older Typhoons", *Janes,* (2021).
G. Allison, "Typhoon Life to Be Extended Two More Squadrons to Be Created", *UK Defence Journal,* (2015).
UK, "Combat Air Strategy: An Ambitious Vision for the Future ", 6.

[910] "Lightening (F35-B) (2021)", ed. Royal Air Force (2021).

[911] For F-35 capabilities, see:
Ibid.
For the 'best fighter in the world' claim, see:
T. Naegele, "The Best Fighter in the World", *Air Force Magazine*, 26 March 2021.

considerably lower number of 48[912]. These figures were reinforced by James Heappey, Minister for the Armed Forces, in March 2021 and Jeremy Quinn, Minister of State at the MOD, in July 2021. Given this, and even factoring in potential reductions in the Typhoon fleet, any aspiration to purchase more than 48 F-35s are unlikely to be achieved[913].

Countering this apparent political clarity, Air Marshal Richard Knighton, the UK MOD senior capabilities Officer, stated on 8 December 2020 that to sustain the F-35 and carrier capability the UK needed to 'increase the number of F-35s that we buy'[914]. Though he acknowledged that 'the precise number and the shape of that profile is, to some extent, dependent on our analysis around the overall future combat air system', he reiterated with clarity that 'we know we will need to order more F-35s'[915].

Further analysed by Bronk, the reality of the UK only purchasing 48 F-35s to operate alongside Typhoon is characterised as troubling. Discussing the fact that as a nation with global aspirations the UK must be able to deliver the full remit of combat air power, he concludes that with only 48 F35s, all of which will be heavily committed to global carrier deployments, the UK is unlikely to deliver in all areas[916]. Reinforcing this, and reflecting on the Typhoon's operational limitations and the intent to remove it from service in the 2030s, Lye concludes that 48 aircraft would at best only allow the UK to generate 12 to 24 platforms to support carrier operations with, in extreme conditions, a total of 36 for short notice surges[917]. With the Queen Elizabeth-Class (QEC) carriers able to carry up to 36 F-35s, or a routine complement of 24, this means that even in periods of surge

[912] A. Goldie, "Joint Strike Fighter Aircraft: Question for Ministry of Defence", ed. UK Parliament (Written Questions, Answers and Statements2020).

[913] For Heappey's statement, see:
J. Heappey, interview by A. Mehta, 23 March 2021.
For Quinn's statement see:
J. Quinn, interview by G. Allison, 27 July 2021.

[914] R. Knighton, interview by House of Commons Defence Committee, 8 December 2020.

[915] Ibid.

[916] Bronk lists the full remit of air combat operations as: suppression of enemy air defenses, penetrating ISTAR and strike.
J. Bronk, interview by A. Mehta, 23 March 2021.

[917] H. Lye, "Uk Mod Civilian Head Cases Doubt on 138 F-35 Fleet Number", *Airforce Technology* (2021).

the UK would be at least 36 aircraft short of supporting its own carrier capabilities at full strength, not to mention other land-based operations[918].

The House of Common's Defence Committee concluded in 2017 that the MOD's lack of transparency on F-35 costs make it increasingly likely that the project would become unaffordable. With this compounded by wider reports that the F-35 programme is financially 'bleeding dry' the participating air forces, the die appears cast. Specifically, the UK under increasing economic pressure will be limited to its current fleet of time restricted Typhoons and 90 less than required F-35s to meet the global air combat power expectations of a 'Global Britain'. With this including the aspirations of a nation able to deliver 'persistent global engagement…[including] constant campaigning', the requirements placed on the pivotal capability of combat air seem set in the short to medium term likely to exceed resources[919]. Leading to a reality in which the UK is unable to meet its self-imposed global role, the outlook for maintaining a residual great-power status through military means appears bleak.

Though the present delta in UK combat air meeting national aspiration is concerning, it is not the first time UK defence has faced such an issue. For example, through the 2010 SDSR the UK's Illustrious Class aircraft carriers and Harrier force were withdrawn from service leaving the UK without an operational carrier strike capability from 2011 to 2021[920]. Now regained through the delivery of the QEC carriers, some argue that the UK's combat air delta will too be regained through the Tempest programme.

Launched as the central element of the UK's 2018 Combat Air Strategy, Tempest has been widely reported as a direct replacement for Typhoon[921]. Though an

[918] Staff Writer, "Hms Queen Elizabeth: All You Need to Know About the Aircraft Carrier", https://www.forces.net/news/hms-queen-elizabeth-all-you-need-know-about-britains-aircraft-carrier.

[919] UK, "Defence in a Competetive Age", ed. Minostry of Defence (2021), 1.

[920] For a background on the Illustrious Class Carriers, see:

C. Parry, "The United Kingdom's Future Carriers: What Are the Good For?", *RUSI Journal,* 157, no. 6 (2012).

For a summary of current UK Carrier Strike and its role, see:

J. Beale, "Hms Queen Elizabeth: Why Is a Uk Aircraft Carrier Going on a World Tour?", *BBC News* 21 May 2021.

[921] Examples of this reporting include:

S. Young, "Uk Set to Sign Contracts with Tempest Partners", *Reuters* 29 September 2021.

R. Davies, "Uk Unveils New Tempest Fighter Jet to Replace Typhoon", *The Guardian* 16 July 2018.

interpretation supported by the RAF in its own statements, the project represents a group of multinational industry and government partners from the UK, Italy, Sweden, and Japan who are collectively working to develop the next generation of combat aircraft technologies[922]. Whilst this is commonly perceived as a manned sixth-generation aircraft that, whilst more advanced, remains similar in context to the F-35 and Typhoon, the actual form Tempest will take remains unclear[923].

Of the options muted to date, commentators have suggested that it may become a 'system of systems' combining a manned platform with unmanned adjunct drones[924]. Operating in tandem and overseen by a human pilot, the supporting drones could act individually or as a 'swarm' to protect the manned aircraft or increase its striking power[925].

This configuration is however far from certain. For example, Royal United Services Institute (RUSI) analysis argues that the core platform is likely to be 'optionally manned' allowing it to fly with or without a human pilot[926]. As this would require the platform to include the significant overheads of life support and physical space for the pilot even when operated unmanned, others go further suggesting that in delivery Tempest will be influenced, and may even merge with, the RAF unmanned Alvina drone programme.

Discussed in 2021 by Air Chief Marshal Sir Mike Wigston, the RAF Chief of the Air Staff until 2023, it was stated that through Alvina the UK has already proved the capability of 'swarms of over 20 ultra-low cost drones operating together

[922] For RAF statements on Tempest, see:
UK, "Tempest Aircraft Concept ", ed. Royal Air Force (2021).
For depth on the Team Tempest concept, see:
"Tempest", ed. Royal Air Force (2021).
For international cooperation in Team Tempest, see:
"Uk and Sweden Partner on Future Combat Air', Defence and Armed Forces News Story", ed. Gov.UK (Defence and Armed Forces News Story 2019).
S. D'Urso, "Italy, United Kingdom and Sweden Sign Tempest Fcas Coordination Memorandum of Understanding", *The Aviationist* (2021).

[923] For a summary of the undefined end state of Tempest and how it may evolve, see:
G. Allison, "What Is the Purpose of Tempest", *UK Defence Journal* (2018).
L. Brooke-Holland, "The Combat Air Strategy: From Typhoon to 'Tempest'?", ed. House of Commons Library (2018).

[924] Price Waterhouse Cooper, "Assessment of the Expected Economic Impact of the Tempest Programme (2021-2050)", (2021), 4.

[925] Brooke-Holland, "The Combat Air Strategy: From Typhoon to 'Tempest'?".

[926] J. Bronk, "Enter the Tempest", *RUSI Defence Systems,* (2018).

against threat systems to brilliant effect'[927]*.* With Wigston further commenting that Alvina would be part of the family of platforms that 'will come together as the Future Combat Air System' and has previously asserted that by 2030 80 percent of UK air power would be unmanned, there is a clear indication that unmanned systems will form a major element of the UK's future air combat capability[928]*.*

Such unmanned platforms, commonly referred to as UCAV, are also likely to offer much more capability than the UK's current fleet of Reaper UCAV, or its successor Protector[929]. By removing previous limitations of poor weather and a constant reliance on uninterrupted digital data links by employing enhanced technologies including AI, the options UCAVs could offer future air forces is considerable*.* Though within this promise the legal and ethical issues of UCAVs are still to be defined, and the technology for fully autonomous UCAVs remaining in development, the potential utility is unquestioned[930].

Given these advantages, and the UK's financial challenges outlined above, it is unsurprising that Tempest appears certain to adopt some form of unmanned swarming and standoff munitions to avoid 'the inescapable trend in previous generations of combat aircraft…where rising demands for lethality and survivability pushed unit cost…resulting in ever-smaller fleet sizes'[931]. Going further, however, and even when it is accepted that investment in Tempest will benefit the UK through the creation of 21,000 jobs in some of its less affluent

[927] Wigston, M. 'Key Note Speech', *Global Air Chiefs Conference,* 14 July (2021). Available at: Global Air Chiefs Conference-CAS Speech.docx (live.com) (Accessed: 1 November 2021).

[928] For Wigston's comment, see:
M. Wigston, "Key Note Speech ", in *Global Air Chiefs Conference* (2021).
For further comment on Alvina, see:
G. Allison, "Raf to Introduce Additional Swarming Drone Squadron", *UK Defence Journal,* (2021).
G. Jennings, "Raf to Expand Swarming Drone Capabilities'", *Janes,* (2021).

[929] For detail on Reaper and Protector, see:
UK, "Reaper (Mq-Ra)", ed. Royal Air Force (2-21).
"Protector (Rg Mk 1)", ed. Royal Air Force (2021).

[930] For the options UCAV may offer, see:
Bronk, "Combat Air Choices for the Uk Government".
For depth on UCAV ethical and legal issues, see:
A.M. Johnson, Axinn, S. , "The Morality of Autonomous Robots", *Journal of Military Ethics* 12, no. 2 (2013).
Beck Bhutam N., S., Geib, R., Liu, H., Claud, K. , *Autonomous Weapon Systems: Law, Ethics and Policy* (Cambridge Cambridge Universitry Press, 2016).
P. Scharre, "Autonomous Weapons and Operational Risk", *Centre for a New American Security,* (2016).
For depth on technical UCAV challenges, see:
E. Sepulveda, Smith, H. , "Technological Challenges of Stealth Unmanned Combat Aerial Vehicles", *The Aeronautical Journal,* 121, no. 1243 (2017).
For depth on UCAV utility, see:
T. Hamilton, Ochmanek, D. , "Operating Low-Cost, Reusable Unmanned Aerial Vehicles", *RAND,* (2020).

[931] Bronk, "Combat Air Choices for the Uk Government".

regions, the logic of unmanned options may force out the manned centre piece of Tempest[932].

This argument is supported by the financial realities. Already having cost the UK £2bn in research and development, critics of Tempest argue that the programme is becoming 'a proverbial black hole'[933]. This assertion was reinforced in 2021 by the National Audit Office (NOA) which 'chastised' the MOD for presenting unaffordable equipment plans four years in a row[934]. Offering detailed figures, the NOA went on to suggest that in the first five years of the MOD's 2020-2030 plan there will be a £8.3bn shortfall with no departmental contingency budget planned to offset any 'unexpected cost increases'[935]. With these comments made after the UK Government boosted the Defence Budget in 2020, some commentators have concluded that the Tempest project, like many other proposed sixth-generation aircraft, is too costly to ever get off the ground if a manned element remains in the plan[936].

Based on the above arguments, it is assessed as likely that if the UK pursues a manned Tempest option, it is likely that by the late 2030s the F-35 and Typhoon fate of reducing platforms will be continued into the Tempest programme. In such a circumstance, the UK would, despite its technological advancements, be unable in not only the short but also medium and long terms to field a combat air capability with sufficient mass to assure its globally inspired residual-great power role. Therefore, faced with the realities of air power forming the backbone of the 'Global Britain' aspirations, it is predicted that the UK's combat air capability will on the retirement of Typhoon in the 2030s consist of 48 manned F-35s focused largely (if not solely) on carrier operations alongside a fleet of unmanned UCAV evolved from the Alvina and Tempest programmes.

[932] Cooper, "Assessment of the Expected Economic Impact of the Tempest Programme (2021-2050)", 7.
[933] P. Suciu, "Tempest: The Revolutionary Stealth Fighter That Might Be Too Expensive", *National Interest,* (2021).
[934] H. Warrell, "Mod Accused of Overspending as Budget 'Black Hole' Hits £17bn", *Financial Times* 21 January 2021.
[935] For the NOA report, see:
UK, "Ministry of Defence - the Equipment Plan 2020 to 2030", ed. National Audit Office (2021).
[936] Staff Writer, "'Defence Funding Boost 'Extends British Influence', Say Pm", *BBC News*, 19 November 2021; S. Roblin, "Some Sixth-Generation Stealth Fighters May Never Get Off the Ground", *National Interest*, 20 April 2021.

Cyber Vulnerabilities of UK Air Power

Reflecting on the above, we find the UK as a residual great power seeking to maintain its constructivist 'Global Britain' role against a backdrop of relative decline across the diplomatic and economic levers of national power. To balance these factors and maintain the national desired relevancy, the UK has routinely sought to achieve advantage through its military. However, also constrained by economic pressures, the UK has adopted a military capability strategy focused on technological advantage over mass.

Considering UK air power specifically, it has been shown how this will by the 2030s translate into the UK's sovereign strike capability being delivered by a much-reduced complement of 48 F-35s alongside a likely fleet of unmanned UCAV. The question for the UK in the context of this thesis is therefore what nature of cyber vulnerabilities this resultant air power capability will be exposed to.

Examining first the F-35, this immensely complex fifth-generation air platform is produced by defence contractor Lockheed-Martin for the US, 7 international partners and 6 other purchasers[937]. With the UK one amongst these, it is immediately evident that despite being a sovereign UK capability, the UK is exposed to not only its own national vulnerabilities but those of the entire programme.

Considering this further, the F-35 is heralded as the West's flagship fifth-generation fighter. Despite this, discussions of its cyber vulnerabilities are long, concerning and widely available in the public domain. Emerging from the fact that the F-35 is entirely reliant on its digital systems, a situation is created in which any serious cyber vulnerability could, if exploited, prevent the platform from taking flight. Within this, the most widely discussed and serious cyber vulnerabilities to date have been reported with the F-35 ground support system, ALIS.

[937] Lockheed-Martin, "The Global F-35 Enterprise ".

Expected to be replaced by an improved option of ODIN, concerns with ALIS have nonetheless plagued all F-35 partners, including the UK. Offering 'a comprehensive logistic support environment', ALIS delivers an array of fully integrated digital systems spanning every element of the aircraft 'from tip to tail'[938]. Making it the 'single, secure information environment…for all elements of F-35 operations', it can be asserted that the loss of ALIS via an exploited cyber vulnerability would mean the loss of the platform. Further, since ALIS is itself networked across not only each flying unit but also each air force and the wider F-35 project via servers at local, national, and international levels, it is plausible that the exploitation of a single cyber vulnerability and the introduction of malware could compromise the entire F-35 fleet[939].

Whilst reporting indicates that improvements have been made to ALIS, and as noted it is due to be replaced by ODIN, the viability of these concerns have been demonstrated. For example, F-35 prime contractor Lockheed-Martin acknowledged in 2015 that a series of sophisticated and successful attacks had occurred against its systems. Furthermore, the US JPO acting on their knowledge of ALIS in 2016 refused to proceed with scheduled cyber tests because of an assessment that realistic 'hacker tools' could compromise and damage the system. Based on this evidence, it can be concluded that through ALIS the F-35 is vulnerable[940].

With the UK only planning to operate 48 F-35s, and with following retirement of the Typhoon and questions over Tempest a real possibility of there being no other manned platforms to replace its strike capability, this conclusion is concerning. If, for example, an ALIS vulnerability were to cause a single F-35 to be grounded

[938] For the quote, see:
Henley et al., "Autonomic Logistics - the Support Concept for the 21st Century'", 417.
For depth, see:
Brissett, "Alis 2.02 Ready to Go".

[939] The unit level ALIS server is referred to as the Squadron Operating Unit (SOU), with the national level server referred to as the Autonomic Logistics Operating Unit (ALOU). Lockheed-Martin, the prime contractor, then operates fleet wide servers.
US, "Observations on the Marine Corps F-35b Demonstration on Uss Wasp: Memorandum for under Secretary of Defense for Acquisition, Technology and Logistics", 1.

[940] For 2015 cyber attacks, see:
Shalal-Esa, "Lockheed's F-35 Logistics System Revolutionary but Risky".
For JPO concerns, see:
Grazier, "F-35 Officials Prove Need for Cyber Testing by Cancelling One".

the UK would in one incident lose a significant percentage of its air power capability. However, given the networked nature of ALIS such a scenario is unlikely. Rather, what is more plausible is that the exploitation of a ALIS vulnerability could compromise at a minimum a squadron of aircraft which are operating from the same local server. If not identified and contained quickly, this could extend to the UK's entire fleet removing a considerable, if not strategically decisive, proportion of UK air power. With this capability pivotal to the maintenance of the UK's 'Global Britain' aspirations, such a loss if not managed, mitigated, and recovered from quickly could, especially in a moment of crisis, cause this residual great power to slip towards regional power status.

Turning next to the second element of the UK's planned air power capability, UCAV, the scenario continues to be of concern. Predicted by Wigston as likely to form 80 percent of UK air power by 2030 when the Tempest and Alvina programmes 'come together as the Future Combat Air System', there is little doubt that UCAVs will form a substantial part of the future UK air power capability[941]. However, with the human removed from the cockpit the platforms become entirely reliant on onboard digital networks and, at least until AI becomes a reality, datalinks, and ground support networks to operate remotely. With at every stage UCAVs susceptible to cyber vulnerabilities, the UK's reliance on the capability introduces uncertainty.

Discussed by Ly and Ly, the options for using cyber means to target UCAV platforms are extensive. Exploring some of the more probable, they highlight the potential for DoS attacks in which an attacker floods a UCAV datalink with enough requests or packets to inhibit communications thereby preventing its effective operation even when links are encrypted[942]. In a further example, they also note how GPS Jamming and Spoofing can prevent a UCAV from receiving a GPS signal or replace that signal with another feed to undermine effective operations[943].

[941] Wigston, "Key Note Speech ".
[942] For a summary of potential DoS attacks on UAVs, see:
Ly, "Cybersecurity in Unmanned Aerial Vehicles (Uavs)", 5.
For further depth, see:
US, "Understanding Denial-of-Service Attacks', Security Tips".
[943] Ly, "Cybersecurity in Unmanned Aerial Vehicles (Uavs)", 5.

When considered against the fleet of current and planned UK UCAVs which will form the future backbone of its air power, the viability of the vulnerabilities outlined by Ly and Ly become evident[944]. Beginning with the longest serving UK UCAV, the US supplied Reaper, we note that the platform came into service in 2007 with the first kinetic strike occurring in May 2008 in Afghanistan[945]. Though persistently operated in the Middle East and North Africa (MENA) region by in-theatre launch and recovery teams, most notably in Afghanistan and against ISIS in Iraq, its 10 Reaper platforms have throughout their service been controlled by human pilots at remote Ground Control Centres (GCC)[946]. Located in Nevada, US, and Lincolnshire, UK, these crews control the Reapers sensors and weapon systems via secure satellite communication systems[947].

Although the UK claims that this operational delivery is managed by secure over-the-horizon datalinks, publicly available examples show that the Reaper can and has been compromised. In terms of the datalinks themselves, events which prove this include 2009 reports of Iraqi insurgents using commercially available Sky Grabber software to compromise and record Reaper video datalinks[948]. Alternatively, the GCCs have also been shown to be vulnerable. For example, in 2011 reporting confirmed that keylogging malware was found on Reaper control systems in the US. Recording every action taken by the crews, it forced the grounding of the entire US fleet of Reapers[949]. Finally, on direct attacks, forced by the Iranian capture of a US Sentinel UAV in 2011, tests commissioned by the USAF and conducted by the University of Texas in 2012 showed how the Reaper could be captured and controlled by spoofing its GPS system[950].

[944] Ibid.

[945] Bureau of Investigative Journalism, "Hc 772 Defence Committee: Written Evidence from the Bureau of Investigative Journalism", ed. UK Parliament (Parliamentary Business 2014).

[946] G. Jennings, "Uk Receives New Reaper Uav to Support Transition to Protector", *Janes,* (2021).

[947] Royal Air Force, "Reaper (Mq09a)", ed. Royal Air Force (2022).

[948] For analysis on the events of the video datalink compromise, see:
D.A. Boutros, "Operational Protection from Unmanned Aerial Systems ", *Joint Military Operations, Naval War College,* (2015): 7.
For depth on Sky Grabber, see:
Arthur, "Skygrabber: The $26 Software Used by Insurgents to Hack into Us Drones".
Software.Informet, "Skygrabber 2.6 ".

[949] For analysis of the keylogging event, see:
Hartmann and Steup, "The Vulnerability of Uavs to Cyber-Attacks; an Approach to the Risk Assessment".
Boutros, "Operational Protection from Unmanned Aerial Systems ", 7.

[950] For the University of Texas study, see:

It is acknowledged that the above examples focus on US Reaper making all dated, especially since the Protector is due to replace Reaper. Notwithstanding this, it is still asserted that they illustrate concerning and likely enduring vulnerabilities that will affect the UK UCAV fleet. Specifically, the examples show how UCAVs can be directly and indirectly targeted via cyber vulnerabilities to either degrade or prevent air operations. Furthermore, it is also noted that with only 10 UK Reapers in operation, and no alternative UCAV platform in service until the introduction of the Protector from 2024, the UK's overall air power capability would be materially threatened if a single Reaper were to be compromised. With the keylogging example also showing how a cyber attack could compromise an entire fleet, a risk heightened by the limited number of UK GCCs, a credible concern emerges that a targeted cyber attack could remove the UK's entire UCAV capability until recovery could occur.

Whilst this argument might be countered by the intent to introduce Protector in 2024 which should have learnt from the cyber vulnerabilities of the Reaper, the UK still only plans to operate 14 Protector platforms whilst phasing out the Reaper fleet. This will mean that, like Reaper, the loss of a single or multiple platforms via cyber attack would have a significant effect on UK air power capability. Furthermore, though it is too early to know how better assured Protector is from cyber attack, the reality remains that without effective AI to remove the requirement for datalinks, all UCAV platforms remain inherently vulnerable to cyber attack.

Reflecting on this, and the above discussions of the UK's F-35, a clear conclusion can be drawn. In its drive to maintain a 'Global Britain' residual Great Power role the UK's investment in technologically advanced aircraft in limited varieties and numbers has created a credible concern. Specifically, with the cyber vulnerabilities shown to be intrinsic to these platforms, there is a credible

A. Kerns, "Unmanned Aircraft Capture and Control Via Gps Spoofing", *Journal of Field Robotics,* 31, no. 4 (2014).

For the Iranian Sentinel UAV incident, see:

F. Gardner, "Why Iran's Capture of Us Drone Will Shake Cia", *BBC News* 8 December 2011.

possibility that they could, against a persistent and capable hostile state adversary, be compromised. If achieved against both types concurrently, the UK could lose its entire air power strike capability. If realised at a strategically critical moment, such a scenario might quickly reduce the UK in stature from a residual great power to a regional power unable to fulfil its 'Global Britain' aspiration.

Looking beyond the platforms themselves, this concern is further underlined by the limited number of bases from which the UK operates its air power. In terms of homeland airfields, for example, the F-35 is operated solely from RAF Marham in Norfolk, UK[951]. With the aircraft reliant on ALIS to conduct operations, relocation of these aircraft to other locations is not a simple or quick task. Therefore, if RAF Marham were to be subject to concerted left-of-launch cyber attacks on its fuels or power systems a hostile actor could prevent the operational utility of the UK's land-based F-35 fleet before flight was even considered.

To counter this, the UK might viably claim that with its two QEC carriers now in service it has created depth and resilience in operational basing. With the carriers also insulated due to their maritime nature from some of the left-of-launch attacks that place land based assets at risk, and with it publicly stated by UK senior Naval Officers that the carriers have been 'built to deal with…[the cyber threats that] we know are there', one might conclude that such confidence is justified[952]. Though possibly the case, and with admittedly little publicly available evidence to question it, some reports have sown concerns.

Taking a 2017 article published in *The Guardian* as an example, it was suggested that the carrier systems were operating the same outdated Windows XP OS that had been targeted by the Wannacry malware. If compromised in such a way, files could be encrypted and systems even crashed making the ship, and therefore the air power it carries, non-operational. Whilst arguably protected by layers of technical security to prevent these events from occurring, all such measures could in a single act be circumnavigated if one of the 700 sailors on board were,

[951] Staff Writer, "F-35b: What You Need to Know About the Lightening Jet", *Forces.net* 17 November 2021.
[952] M. Utley, interview by D. Winder, 21 October 2018.

through subversion, to act as a malicious insider and directly introduce malware onto the ships systems[953]. In such circumstances, half of the UK's maritime air power capability could be taken out of service in moments.

Considered alongside the previous assertion on the UK's reducing options for the delivery of kinetic air power, the realities of the UK's limited operational locations reinforce the conclusion. Specifically, if faced by a determined hostile state actor the UK could at speed lose its air power capability through the cyber compromise of either a single carrier, air base or fleet. With such an adversary likely to target all simultaneously via a combination of technical attacks and the subversion of personnel, the likelihood of a vulnerability being identified and exploited increases. Without sufficient depth in a larger number of platforms and locations to mitigate this, the thesis returns to the conclusion that the UK could through one or a combination of cyber vulnerabilities quickly lose the global relevance it strives to maintain.

Conclusions on UK Air Power Cyber Vulnerabilities

Charting the UK's decline from a superpower to a residual great power, the above discussion explored how the military lever is being used to mitigate further relative decline. Identifying air power as an essential component in this intent, it was highlighted how, despite investment in advanced technologies, the UK continues to struggle to achieve sufficient mass to assure its current role.

Exploring this reality in the context of cyber vulnerabilities, significant concerns across the UK's F-35 and UCAV fleets were identified. Noting how a single exploitation of these could significantly undermine the relatively small UK air power capability, it is asserted that the state is one or two successful cyber attacks away from failing to meet its role-based commitments. The cyber vulnerabilities of UK air power are therefore concluded as not only a technical or military issue. Rather, if the UK is to remain a residual great power with global

[953] Staff Writer, "Hms Queen Elizabeth: All You Need to Know About the Aircraft Carrier", *Forces.net*, 23 May 2021.

relevance, these cyber vulnerabilities must be considered a national concern with strategic implications.

Taiwan: Western Aligned Regional Power

Introduction to Taiwanese Air Power's Cyber Vulnerabilities

In the final discussion of cyber vulnerabilities, this section will discuss the regional power of Taiwan. Though potentially viewed as an unusual choice given the Western focus of Part 2 of the thesis, this island nation offers a relevant and valuable case study as justified through two factors. Firstly, aligned with the US and in conflict with the PRC, Taiwan is firmly in the Western sphere of influence. Secondly, though Taiwan is acknowledged as not being in the traditional regional power ilk, it maintains a significant military capability in a bid to deter a much larger aggressive neighbour. In the context of these factors, Taiwan has relevance to this discussion by personifying the challenges faced by other Western and Western-aligned states with regionally bounded interests.

Based on this, the section will open by exploring Taiwan's development towards becoming a fiercely independent state with far greater geopolitical importance than its size suggests. Having charted this development, the section will next discuss how the Taiwanese military, the strategic approach it has employed and the US assurances it has held have combined to deter a forcible reunification with the PRC. Expanded on by a focused consideration of Taiwanese air power, it will be shown how a large fleet of fourth-generation F-16Vs is now pitched against improving PRC air power capabilities.

Developing the impact of this situation with reference to cyber vulnerabilities of Taiwanese air power, the section will consider the F-16 itself before exploring wider indirect concerns. Taken collectively, it will be concluded that the PRC is likely to undermine Taiwanese air power through cyber means. Given this, and the existential threat it faces if cyber vulnerabilities have this impact, Taiwan's cyber concerns will be argued as the most pressing of all the states considered in this Chapter.

Taiwan: Geographically Small, but Geopolitically Pivotal

Located 100 miles off the PRC's southeast coast, the island of Taiwan with a population of 23 million is at 36,000 square kilometres roughly the size of Belgium[954]. Though currently recognised as a state under its formal name of the Republic of China (ROC) by only 17 countries and dwarfed by a neighbour which poses it a credible existential threat, Taiwan's complicated history and enduring US support have made it more geopolitically important than its size suggests[955]. This has also established a deeply ingrained national role and identity built on a fierce sense of independence.

To explore this role, it is instructive to look back at the development and establishment of the modern nation of Taiwan. In doing so it can be recognised how people with links to Austronesian cultures have inhabited the island for an uncharted period. Further, it can also be noted that from the advent of historical records expeditions from the Chinese mainland had explored the island as early as the 3rd century. However, in charting the development of contemporary Taiwan's character and role, it is most intuitive to divide its history into 5 distinct periods beginning in the 17th century[956].

Considering the first period, we find that from 1624 the Dutch East India Company began its colonisation in south-western Taiwan before spreading across the island. Seeking to capitalise on Taiwan's natural resources but short of indigenous labour, the Dutch encouraged Chinese immigration. Instigating the first large-scale Chinese migration to the island, the action would establish an enduring cultural linkage with the Chinese mainland[957].

[954] C. Textor, "Taiwan - Statistics and Facts ", (Statistica, 2001).
[955] C. Horton, "Taiwan's Status Is a Geopolitical Absurdity", *The Atlantic,* (2019).
[956] For a summary of the Taiwanese Austronesian cultural origins, see:
P Bellwood, Dixon.E., "Austronesian Cultural Origins: Out of Taiwan, Via the Batanes Islands, and Onwards to Western Polynesia," in *Past Human Migrations in East Asia* (New York: Routledge, 2008).
[957] For depth on the Dutch control of Taiwan and the requirement to induce Chinese immigration, see:
T. Andrade, "The Rise and Fall of Dutch Taiwan, 1624–1662: Cooperative Colonization and the Statist Model of European Expansion", *Journal of World History* 17, no. 4 (2006).

First established in the early 17th century, these linkages would grow and formalise in the second phase of Taiwanese development under the Zheng regime from 1662. Established through the Ming Dynasty's search for a location to regroup following its defeat by the Qing Dynasty, the remaining Ming leadership under Zheng Cheng-gong chose to fight the Dutch and claim Taiwan for their own purposes. Taking Fort Zeelandia in 1662 and forcing the Dutch to withdraw, Zheng Cheng-gong and later his son would impose a Chinese style administration on the island. When combined with the increased migration from mainland China that would follow, the island's society became dominated by Southern-Min Chinese. Reinforcing the Chinese cultural identity over top of the indigenous Taiwanese peoples, an identification with China, but one forged in conflict and division with those remaining on the mainland, would be created[958].

Despite the Zengh regime prospering, it would be defeated by the Qing Dynasty in 1683. Ushering in the third phase of Taiwanese development, the shift would for the first time formally bring the island under sovereign control of the Chinese mainland. Part of a much wider expansionism pursued by the Qinq Dynasty in this period which included new frontiers including Tibet and Xinjiang, Taiwan was not unique in its inclusion under Qing sovereign control. However, what makes this period particularly pivotal to the contemporary Taiwanese role and character is twofold. Firstly, the migration from mainland China that followed Qing control further underpinned the islands' Chinese cultural identity. Secondly, and perhaps most pivotal, the PRC currently claims sovereignty over virtually all territories acquired by the Qing Dynasty. With the PRC also labelling any separatist movements illegitimate regardless of interceding historical events, the period becomes one of, if not the, most historically influential in the development of current Taiwanese geopolitics[959].

[958] For depth on Zheng Cheng-gong's removal of the Dutch from Taiwan and subsequent rule, see:
How Taiwan Became Chinese: Dutch, Spanish, and Han Colonization in the Seventeenth Century (New York: Columbia Unveristy Press, 2010).

[959] For depth on the Qing Dynasty control of Taiwan, see:
J. Teng, "Taiwan in the Chinese Imagination, 17th-19th Centuries", *The Asia-Pacific Journal,* 5, no. 6 (2007).

Chinese mainland rule over Taiwan would end in 1895. Caused by the defeat of China in the First Sino-Japanese War, the Treaty of Shimonoseki saw the islands ceded to the Empire of Japan allowing the fourth period of Taiwanese development to begin[960]. Following the transition, the new Japanese rulers attempted to cement their control through a policy of assimilation towards the island's inhabitants. Intended to make Taiwan and its people a formal and cultural extension of the Japanese home islands, such transition was resisted by a population who because of the preceding centuries remained culturally Chinese. Leading to events such as the Wushe Uprising in 1930 in which Japan mobilised 3,000 troops to kill 214 Seediq warriors and their families, tensions continued throughout Japanese colonial rule[961]. Reflecting on this, it becomes evident that whilst passing between rulers and never once being self-governed, the spirit of the Taiwanese population to be both Chinese by culture but distinct from those who try to dominate them had established itself in the island's psyche.

Leading to the fifth and final phase of Taiwan's development, this drive for self-determination would be fostered by new arrivals who like Zheng Cheng-gong sought shelter from forces dominating mainland China. Beginning in 1945 after the defeat of Japan, the island would initially be controlled by the mainland Chinese ROC on behalf of the Allies. However, the situation would be short lived when in 1949 civil war broke out in China and troops loyal to the ROC's leader, Chiang Kai-shek, were pushed back by Mao Zedong's communist forces. Forcing Chiang and his Chinese Nationalist Party or Kuomintang (KMT) government to flee to Taiwan, they sought control of the island establishing a divide with the mainland that has endured into the 21st century[962].

In reflecting on the KMT's move to the island, and the reestablishment of the ROC as a political entity on the island of Taiwan with aspirations to return to the mainland, the impact was not only internationally but domestically significant.

[960] For depth on The Treaty of Shimonoseki and the ceding of Taiwan to Japan, see:
Z. Haipeng, Guoqiang, L., "The Treaty of Shimonoseki, the Diaoyu Islands and the Ryukyu Issue", *International Critical Thought,* 7, no. 1 (2017).

[961] For depth on Taiwanese-Japanese tensions and the Wushe Uprising, see:
T.J. Ward, Lay, W.D., "The Unusual Case of Taiwan", *e-International Relations,* (2019).

[962] For the KMT withdrawal from mainland China, see:
11-26D. Roy, *Taiwan: A Political History* (Ithaca: Cornell University Press 2003).

Creating not just a political and military divide with the mainland, the group's followers who would only number approximately 1.5 million or 14 percent of the island's population quickly came to dominate Taiwanese politics. Establishing an authoritarian regime, the KMT may have evolved from their Leninist routes by the 1950s but in their rule, they retained an ideology based on centralism[963]. This would remain the driving principle behind Taiwanese governance until Chiang's son, Chiang Ching-kuo, finally introduced a process of democratisation that in 2000 led to the election of the island's first non-KMT elected president, Chen Shui-bian[964].

It is notable that against this backdrop of the KMT split from mainland China and democratic developments, improvements in Chinese-Taiwanese relations did occur in the 1980s. However, what never diminished was the mainland claim that Taiwan had from the Qing Dynasty onwards been a rightful part of the PRC. Within this, the PRC would also develop and maintain its overt drive to establish a One Country, Two Systems (OCTS) policy. Through this Taiwan would, if it agreed to reunification, maintain its capitalist processes whilst becoming a 'special administrative region with a high degree of autonomy' in executive, legislative and judicial matters[965]. However, with Hong Kong touted as a showcase of this policy, and the increasingly authoritarian PRC control of Hong Kong leading the Taiwanese President Taei Ing-wen to describe it as the 'edge of disorder', OCTS has been firmly rejected by the Taiwanese people who retain their fiercely independent character[966].

Such independent drive has not diminished the PRC intent with in 2015 the Anti-Secession Law passed by the Third Session of the Tenth National People's Congress making their position unmoveable. Stating in Article 1 that the PRC

[963] B.J. Dickson, "The Lessons of Defeat: The Reorganization of the Kuomintang on Taiwan, 1950-52", *The China Quarterly,* 133 (1993).

[964] For a timeline of Taiwanese political development, see:
Reuters Staff, "Timeline: Taiwan's Road to Democracy", *Reuters* 13 December 2011.

[965] S. Cooney, "Why Taiwan Is Not Hong Kong: A Review of the Prc's "One Country Two Systems" Model for Reunification with Taiwan ", *Washington Journal of Law,* 6, no. 3 (1997).

[966] For depth on the failure of OCTS, see:
W.H. Overholt, "Hong Kong: The Rise and Fall of 'One Country, Two Systems'", *Ash Center for Democratic Governance , University of Harvard* (2019).
For President Taei Ing-wen's comments, see:
Y. Lee, "Taiwan Leader Rejects China's 'One Country, Two Systems' Offer", *Reuters* 10 October 2019.

opposes 'Taiwan's secession from China by secessionists in the name of Taiwan independence', the Law goes on in Article 2 to crystallise the PRC's position. Specifically, it states that 'Taiwan is part of China…[and that] the state shall never allow the 'Taiwan independence' secessionist forces to make Taiwan secede from China under any name or by any means'[967].

Given the considerable difference in size and power of the PRC and Taiwan, and the fact that Taiwan is diplomatically recognised by only 13 states, it might be expected that the reunification of the island with the mainland is an inevitability regardless of what role and character the island may hold[968]. However, despite Taiwan not having formal diplomatic relations with major powers, the US has maintained a strong and supportive relationship. Initially in the form of the US-Taiwanese mutual defence treaty which existed from 1954, this was replaced in 1979 by the Taiwanese Relation's Act. Though watered down by US President Carter's Administration in exchange for establishing relations with the PRC, the Act retains a broad and deep security relationship. As a result, the Taiwanese military enjoys substantial US arms sales and regular liaison with US forces[969].

Though this relationship remains strong, it also involves a significant level of 'strategic ambiguity'. In this the US asserts that its commitment to Taiwan is 'rock solid' whilst being purposefully vague on whether that support would extend to militarily defending Taiwan in the event of a PRC attack[970].

Whilst the US's conventional military power outweighed that of the PRC, this ambiguity had value. However, with the PRC continuing to strive towards a 'great rejuvenation of the Chinese nation' and an associated aim to surpass global US power, it is quickly closing the gap on US military dominance[971]. Augmented by

[967] People's Republic of China, "Anti-Secession Law", ed. National People's Congres (2015).

[968] Taiwan was in 2021 diplomatically recognised by Belize, eSwatini, Guatemala, Haiti, the Holy See, Honduras, the Marshall Islands, Nauru, Palau, Paraguay, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, and Tuvalu. This has, however, reduced to 13 in 2023.

Stafff Writer, "Who Are Taiwan's Diplomatic Allies?", *Al Jazeera* 10 December 2021.

[969] R. Bush, "The United States Security Partnership with Taiwan"", *The Brookings Institute,* (2016).

[970] For the US statement in support of Taiwan, see:

J. Biden, interview by BBS News, 25 January 2021.

For an overview of 'strategic ambiguity', see:

C. Clark, "The Taiwan Relations Act and the U.S. Balancing Role in Cross-Strait Relations", *American Journal of Chinese Studies,* 17, no. 1 (2010): 14.

[971] US, "Military and Security Developments Involving the People's Republic of China - Annual Report to Congress", iii.

growing non-conventional strengths, some argue that the potential of the PRC military reclaiming Taiwan is growing[972]. For example, US Admiral John Aquilino, Commander of the US Military Indo-Pacific Command, succinctly made this point stating that in the current environment a PRC invasion of Taiwan 'is much closer to us than most think'[973].

Reflecting on the development of Taiwan, its cultural ties to the Chinese mainland, the existential threat to its sovereignty and the existence of US guarantees, the island's geopolitical importance becomes much more significant than its size suggests. Through this, the island's constructivist identity which is set as a regional power fiercely set on assuring its sovereign independence becomes not only important to the nation but to broader global strategic balances of power. Given this, and the militarily charged nature of the situation, the question becomes whether it has the capability to deter, defeat or delay potential PRC aggression whilst it waits for the Western military support that strategically ambiguous assurances from the US suggest it might receive.

Taiwan's Military Instrument: Assured Asymmetry to an Uncertain New Strategy

In considering this question of whether Taiwan can deter or defeat PRC aggression, it is informative to explore the development of its military and concurrent US assurances against PRC aggression. Together these offer an understanding of the military viability of defending the island alongside a baseline on the importance of Taiwanese air power. From there, an assessment of Taiwan's air powers cyber vulnerabilities, and whether these are a pivotal factor in the survival of Taiwanese independence, can be made.

In conducting this review, it is necessary to begin in the 1950s when just after the KMT took control a strategy of forward defence was adopted. Symbolic of the intent to retake the mainland, it focused on occupying and holding islands in the

[972] For a summary of the interplay between PRC and Russian intent, see:
T. Wong, "China: What Does It Want from the Ukraine Crisis with Russia?", *BBC News* 4 February 2022.
[973] J. Aquilino, interview by Staff Writer, 23 March 2021.

Taiwan Strait to be used as a defensive perimeter and a staging post for reinvasion[974]. Despite resourcing the strategy with one third of Taiwan's troops, the islands proximity to the mainland made holding them precarious and dependent on US military support. Forming the first iteration in the 'golden thread' of US military support to Taiwan, this was, despite its importance, not initially assured. Of note, disillusioned with KMT corruption the Truman Administration's 'Statement on Formosa' in January 1950 asserted that it would not use 'its Armed Forces to interfere' on behalf of either the PRC or Taiwan[975].

The outbreak of war in Korea in June 1950 would however change the US's strategic calculus[976]. Intent on preventing communism spreading south, the USN Seventh Fleet was deployed into the Taiwan Strait. In response, the PRC shifted troops poised to invade Taiwan to the Korean front. In combination these events not only delayed the possibility of a PRC invasion but reinvigorated US assurances to Taiwan[977].

Building on this the US Government would in the 1950s reaffirm its support to Taiwan through examples including the Southeast Asia Treaty Organisation (SEATO)[978]. Responded to by increased PRC bombardment of Taiwanese held

[974] For a summary of the 1950s forward defence strategy, see:
M Edmonds, Tsai, M.M., *Defending Taiwan: The Future Vision of Taiwan's Defence Policy and Military Strategy* (New York: Routledge, 2003), 6.
A. Huan, Hui, T.M., "Kinmen at a Crossroads: A Balancing Act? ", (Rajaratnam School of International Sudies 2019).

[975] For the Statement on Formosa, see:
US, "Statement on Formosa", ed. US State Department (1950).
For analysis on the Statement on Formosa, see:
H. Matsumoto, "The First Taiwan Strait Crisis and China's" Border" Dispute around Taiwan ", *Eurasia Border Review,* 3 (2012): 78.
For a further important statement on the lack of guaranteed support from the US to Taiwan, see:
D. Acheson, "Dean Acheson's Speech to the National Press Club ", news release, 1950, https://web.viu.ca/davies/H102/Acheson.speech1950.htm.

[976] For depth on the origins and conduct of the Korean War, see:
S. Sandler, *The Korean War: No Victory, No Victors, No Vanquished* (Kentucky Kentucky University Press 1999).
For the impact of the Korean War on Taiwan, see:
Matsumoto, "The First Taiwan Strait Crisis and China's" Border" Dispute around Taiwan ", 78.

[977] For an overview of these shifts because of the Korean War, see:
US, "The Taiwan Straits Crises: 1954–55 and 1958", ed. The Office of the Historian (2022).

[978] Commonly referred to as the Manila Pact, SEATO was a US led group established to protect the Western Pacific region from communist expansionism. Though dismissed by some historians as a footnote in the Cold War, the PRC considered it a credible threat making its creation a significant strategic moment. For assessments of the impact of SEATO, see:
"Southeast Asia Treaty Organization (Seato), 1954", ed. Office of the Historian (2022).
J.K. Franklin, "The Hollow Pact: Pacific Security and the Southeast Asia Treaty Organization" (Texas Christian University, 2006).
For a representative assessment that SEATO was merely a 'footnote' in the Cold War, see:
J. Cable, *The Geneva Conference of 1954 on Indochina* (New York: St. Martin's Press, 1986), 169.

islands in the Strait, actions which were countered by further US guarantees including the 1955 'Formosa Resolution', the US dimension was established as a guiding light for all future Taiwanese strategic thinking[979].

Continuing into the 1960s and 70s the pivotal nature of US military support would again be reaffirmed. For example, emboldened by the internal PRC chaos unleashed by the 'Great Leap Forward', Chiang Kai-shek saw an opportunity to 'Retake the Mainland'[980]. However, lacking the military ability to achieve this domestically, and refused support by the Kennedy Administration, Chiang Kai-shek was forced to abandon his plans demonstrating how Taiwan was both offensively and defensively dependant on the US[981].

This assertion would be further reinforced in 1979 with the removal of the US-Taiwanese Mutual Defence Agreement and the creation of the US Taiwan Relations Act[982]. Combining to create the US's ongoing 'strategic ambiguity' towards Taiwan in which the degree it would intervene against PRC aggression was made purposefully unclear, this US 'golden thread' would finally reinforce the Taiwanese strategic position. Specifically, Taiwan has since 1979 focused on politically resisting unification whilst concurrently being ready to defend the island militarily with an expectation of US support[983].

[979] For detail on the PRC bombardment of Taiwanese held islands, events commonly referred to as the Taiwan Strait Crisis, and the 'Formosa Resolution' which offered US President Eisenhower total authority to defend Taiwan and its offshore islands against communist attack, see:

US, "The Taiwan Straits Crises: 1954–55 and 1958".

[980] The 'Great Leap Forward' was a radical campaign launched from 1958 by the PRC's Chairman Mao to outproduce the old colonial power of the UK while simultaneously achieving Communism. Beset by unrealistic goals and widespread fraud the 'Leap' resulted in the starvation of one in 20 of the Chinese population. For depth on the 'Leap', see:

C.D. Brown, "China's Great Leap Forward", *Asian Studies* 17, no. 3 (2012).

For a discussion of Chiang Kai-shek's intent to 'Retake the Mainland', see:

T. Igarashi, "When Did the Roc Abandon "Retaking the Mainland"? The Transformation of Military Strategy in Taiwan", *Journal of Contemporary East Asia Studies,* 10, no. 1 (2021): 138.

[981] For depth on the Kennedy Administrations decision and its impact on Taiwanese strategic thinking, see:

"When Did the Roc Abandon "Retaking the Mainland"? The Transformation of Military Strategy in Taiwan", 138.

US, "Chinese Nationalist Maritime Activities against the China Mainland", ed. National Security Archive (1962).

"Foreign Relations of the United States and China, 1964–1968", ed. Office of the Historian (2022).

[982] For depth on these developments, see:

Edmonds, *Defending Taiwan: The Future Vision of Taiwan's Defence Policy and Military Strategy*, 6.

[983] For a discussion of this shift in the Taiwanese strategic calculus, see:

Igarashi, "When Did the Roc Abandon "Retaking the Mainland"? The Transformation of Military Strategy in Taiwan", 138.

Transitioning into the post-Cold War, this strategic calculus has despite regular shifts in US-Sino relations remained consistent[984]. Beginning in 1988 under President Lee Teng-hui's 'resolute defense, effective deterrence', and developed in 2000 with President Chen Shui-bian's amended but strategically consistent 'effective deterrence and strong defense', little changed in Taiwan's fundamental approach[985]. Notably, it continued to focus on convincing the PRC that it would extract a heavy price for any attempt to cross the Strait[986].

Moving into the contemporary space, this entrenched strategy was underlined in 2017 by the Overall Defence Concept (ODC)[987]. Supported by increasing defence budgets, ODC refreshed the previous strategies by identifying Taiwan's air and maritime assets as key to undermining the PRCs ability to cross the Strait[988]. This would be followed by Taiwanese attacks on PRC beachheads using light assets such as mine layers, swarms of small fast attack boats and truck-launched anti-ship cruise missiles[989]. By doing so in an asymmetric manner, ODC did not seek to compete with the PRC head on but target the greatest threats, while surviving long enough for US intervention[990].

[984] Examples of shifting US-Sino relations from the end of the Cold War into the 21st century included:

A high point in cooperation under President Bush in 1989 which threatened a lessening of the US commitment for Taiwan. For depth, see:

J.F. Kornberg, "Comprehensive Engagement: New Frameworks for Sino-American Relations ", *The Journal of East Asian Affairs,* 10, no. 1 (1996): 15.

The significant deterioration in relations after the Tiananmen Square protests in June 1989 and the PRC's reaction to them. For depth, see:

Staff Writer, "Tiananmen Square: What Happened in the Protests of 1989?", *BBC News*, 23 December 2021.

A lessening of the post-Tiananmen Square US sanctions in recognition that that the US needed PRC support in the UNSC ahead of the 1990 Iraq War. For depth, see:

Kornberg, "Comprehensive Engagement: New Frameworks for Sino-American Relations ", 15.

The Clinton Administration's lack of interest in the Asia-Pacific region leading to renewed concerns that US commitments to Taiwan were waning. For depth, see:

Ibid., 19.

W. Lord, "Testimony for the Senate Foreign Relations Committee, Asia and Pacific Subcommittee by Winston Lord, Assistant Secretary for East Asian and Pacific Affairs, Department of State", ed. US Department of State (Archive 1995).

The President G.W. Bush Administration's recognition of the PRC as a 'strategic competitor' which reinforced US support for Taiwan. For depth, see:

Edmonds, *Defending Taiwan: The Future Vision of Taiwan's Defence Policy and Military Strategy*, 3.

[985] For a discussion of President Lee Teng-hui's 1988 'resolute defense, effective deterrence' and President Chen Shui-bian's 2000 'effective deterrence and strong defense', see:

Defending Taiwan: The Future Vision of Taiwan's Defence Policy and Military Strategy, 6.

[986] Ibid., 8.

[987] E.. Hsi-min Lee, L., "Taiwan's Overall Defense Concept, Explained", *The Diplomat,* (2010).

[988] For detail on the 2019 Taiwanese defence budget, see:

CNA, "National Defense Budget Was Greatly Increased to 358 Billion", (2019).

For a discussion of and an assessed figure on the 2019 PRC defence budget, see:

US, "Keynote Address by Secretary of Defense Mark T. Esper at the Reagan National Defense Forum", ed. US Department of Defense (2019).

[989] D. Thompson, "Hope on the Horizon: Tawian's Radical New Defense ", *War on the Rocks* (2018).

[990] Ibid.

This progression from 'resolute defense, effective deterrence' to ODC assured Taiwanese security into the 21st century indicates a move away from these strategic foundations. Encouraged by increased US commitments to defending Taiwan including the Trump Administrations Taiwan Allies International Protection and Enhance Initiative (TAIPEI) Act and the Biden Administrations statements of 'rock solid' support, it has been suggested that the asymmetric ODC approach will be abandoned[991].

In its place Taiwan's Ministry of National Defense is now thought to be forming plans to deter a PRC invasion by threatening retaliation through missile strikes against the PRC mainland. This will be paired with committing its armed forces to direct combat against a qualitatively and quantitatively superior PLA[992]. Though this runs counter to the Taiwanese Tsai Administration's other national defence reforms, and Taiwan's own assessment that the PRC possesses the ability to paralyse its anti-air and anti-surface systems through 'soft and hard attacks', the shift back towards a 1950s style of approach seems set to continue[993].

Summarised by Hunzeker, it is believed that Taiwan will deliver the military capabilities these new plans demand through increased Defence budgets and US arms deals which are updating obsolete capabilities. In doing so, Taiwan will procure an improved fleet of US-made fighter aircraft, ships, and tanks to offset the PRC's numerical advantages[994]. These would then achieve a sufficient delaying effect for US reinforcements to arrive and ultimately repel further PRC aggression.

[991] The TAIPEI Act signed in 2019 by US President Trump stated that the US would 'increase its economic, security, and diplomatic engagement with nations that have demonstrably strengthened, enhanced, or upgraded relations with Taiwan'. For detail on the Act, see:

US, "Taiwan Allies International Protection and Enhance Initiative (Taipei) Act ", ed. US Congress (2019).

For the PRC's action to entice diplomatic allies away from Taiwan, see:

T.J. Shattuck, "The Race to Zero?: China's Poaching of Taiwan's Diplomatic Allies", *Orbis,* 64, no. 2 (2020).

[991] For Biden's 'rock solid' statement on Taiwan at an Asian Leaders Conference in October 2021, see:

J. Biden, 27 October 2021.

[992] M.A. Hunzeker, "Taiwan's Defense Plans Are Going Off the Rails ", *War on the Rocks,* (2021).

[993] For a summary and assessment of the Taiwanese Ministry of National Defense 2021 PLA Capability Report, see:

Editorial, "Pla Report Sobering, but Accurate", *Taipei Times*, 3 September 2021.

For President Tsai's comments on changes to the use of military reserves, see her May 20 Inaugural Address.

I. Tsai, "Inaugural Address of Roc 15th-Term President Tsai Ing-Wen", ed. President of Taiwan (2020).

[994] Hunzeker, "Taiwan's Defense Plans Are Going Off the Rails ".

Considered in this context, the Taiwanese shift away from ODC asymmetry could be militarily disastrous. With its capabilities improving but remaining in many areas outdated, and the guarantee of US intervention even with recent rhetoric remaining ambiguous, the PRC may be offered sufficient confidence to pursue reunification by force. Given this, and the importance of air power in any attempted invasion of Taiwan, it is necessary to take a deeper look at the role of Taiwanese air power in balancing the strategic scales.

Taiwanese Air Power: Shifting Air Superiority over the Straits of Taiwan

Separated from mainland China by the 100 miles wide Strait of Taiwan, defence of the island is through geographical realities focused on air and maritime power. Though both are essential, and Taiwan continues to invest in key maritime assets such as its indigenous submarine programme, tacticians have long agreed that the reach and speed of air power remains central to any defence of the island from PRC aggression[995].

An assessment embraced early in its military tensions with the PRC, Taiwan's initial strategy of perimeter defence was ably supported by advanced air power that outmatch the PRC. Maintained throughout the 1950s and 60s by large US military sales, the Taiwanese armed forces operated the best aircraft and surface-to-air missiles available[996]. However, on the termination of the Mutual Defence Agreement and creation of the Taiwan Relations Act in 1979 the situation materially changed[997].

With the transition also ending formal diplomatic ties with the US, obtaining military equipment became increasingly difficult for Taiwan. Though the joint US-China Communique signed on 17 August 1982 which limited US arms sales to the island was never fully implemented, the shift was gradually felt as Taiwan's

[995] For the importance of air power in a PRC invasion of Taiwan, see the scenario presented in:
D. Lague, Murray, M., "T-Day: The Battle for Taiwan ", *Reuters Investigates* (2021).
For detail of the Taiwanese submarine programme, see:
D. Cheng, "Taiwan's F-16v Fighter Jet Purchase: Why It Matters", *The Heritage Foundation,* (2020).

[996] Edmonds, *Defending Taiwan: The Future Vision of Taiwan's Defence Policy and Military Strategy*, 6.

[997] Ibid.

military equipment aged into obsolescence through the 1980s[998]. Though seen in all areas, the most acute impact was experienced in the technologically reliant air domain. Unable to update its fighter fleet Taiwan was by the late 1980s restricted to operating platforms such as the 1960s F-4[999].

Recognising the perils of being outmatched by the PRC, Taiwan in parallel to the advent of its 1988 'resolute defense, effective deterrence' strategy actively pursued means of redressing the capability balance and developing a viable deterrence. Whilst the use of maritime to control sea lanes formed a key part of this, 'resolute defense, effective deterrence' notably identified the importance of air power. Highlighted as the only 'reliable countermeasure weapon' with the speed and reach to have decisive impact, air capabilities were seen as essential in both deterring the PRC and holding their advance until US support could arrive. However, with the PLAAF modernising through the 1980s with the introduction of platforms such as the Su-27, it was clear that Taiwan was with its 1960s era air power in no position to enact the strategy[1000]. The drive for modernising Taiwanese air power therefore became central to the 'resolute defense, effective deterrence' strategy[1001].

Still hampered by the restrictions of the Taiwan Relations Act and the US-China Communique, President GHW Bush's faltering 1992 re-election campaign offered Taiwan a lifeline. Leading Bush to court the conservative vote, he abandoned the direction of his Asia-Pacific policy and agreed to sell 145 F-16A/B fighters to Taiwan[1002]. Though this would sour US-Sino relations and fail to guarantee Bush's re-election, the purchase which was pursued alongside the procurement of 57 Mirage 2000D/E fighters and 126 domestically developed Ching-Kuo multirole Indigenous Defence Fighters (IDF) offered Taiwan the air power uplift its strategy required[1003]. Through this Taiwan had by the early 2000s

[998] Ibid.
[999] Ibid.
[1000] Cheng, "Taiwan's F-16v Fighter Jet Purchase: Why It Matters".
[1001] Edmonds, *Defending Taiwan: The Future Vision of Taiwan's Defence Policy and Military Strategy*, 8.
[1002] For a discussion of President G.H.W. Bush's failed re-election campaign, see:
J. Kelly, "George Hw Bush: What Makes a One-Term President?", *BBC News* 2 December 2018.
[1003] For the impact on US-Sino relations, see:
Kornberg, "Comprehensive Engagement: New Frameworks for Sino-American Relations ", 15.
For details on the Taiwanese procurement of the F-16, Mirage and IDF in the 1990s, see:

finally managed to again outmatch PRC air power. In doing so it assured the viability of 'resolute defense, effective deterrence' and its 2000 replacement strategy 'effective deterrence and strong defense'[1004].

In response to this, the PLAAF has since 2000 made a 'great leap forward' in its air power capability[1005]. Shifting from largely obsolete licence-built second and third generation Soviet combat aircraft to a range of modern variants, it has over the last two decades developed a fleet of fourth verging on fifth generation platforms[1006]. Routinely imitating cutting-edge US air power in doing so, developments have included examples such as the Xian Aircraft Corporation's Y-20 transport aircraft modelled on the Boeing C-17, and Chengdu Aerospace Corporation's J-20 modelled on the Lockheed-Martin F-35[1007]. Given the PRC's ability to transform the PLAAF into a world-class air force, there is little doubt that the Taiwanese air force which continues to operate the fleet it procured in the 1990s has become both qualitatively and quantitatively outclassed.

Seeking to repeat the advantages enjoyed in the 1960s and 90s, Taiwan again turned to the US to redress the balance. Taking a new tact, however, Shen Yi-ming, the Taiwanese Deputy Minister of National Defense, confirmed in 2019 that rather than requesting a specific aircraft Taiwan had asked the US to advise on the type and number of fighter jets it required to meet the operational need. A policy confirmed by Major General Tang Hung-an, Head of the Taiwanese Air Force Planning Division, it was commented that the F-15, F-18, F-16 and even the F-35 were among the options Taiwan would consider 'as long as the jets help to strengthen [Taiwanese] air defense capabilities'[1008].

M. Thim, *Taiwan's Air Force: Inventory and Procurement Options*, Taiwan in Perspective (2013).
For depth on the Taiwanese procurement of the F016A/B, see:
T.C. Lee, "Perspectives on Us Salesa of F-16 to Taiwan ", *The Journal of Contemporary China* 2, no. 1 (1993).

[1004] R. Joe, "Anatomy of a Taiwan Invasion: The Air Domain", *The Diplomat,* (2019).

[1005] For this assessment of PRC air power's 'leap forward', see:
J.A. Tirpak, "The Chinese Air Force's Great Leap Forward", *Air Force Magazine,* (2018).

[1006] Ibid.

[1007] For an overview of the Y-20 transport aircraft, see:
J. Bennett, "China's New Y-20 Is the Largest Military Aircraft Currently in Production", *Popular Mechanics,* (2016).
For an overview of the J-20 fighter aircraft and its operational utility, see:
Staff Writer, "Can China's J-20 Fighter Match up with America's F-35 Lightning Ii?", *The National Interest,* (2021).

[1008] For both Shen Yi-ming and Major General Tang Hung-an's comments, see:
M. Yeo, "Taiwan Requests Fighter Jets from the Us, but with an Unusual Twist", *Defence News*, 11 March 2019.

In advance of this request Taiwanese officials including Yen Teh-fa, Minister of National Defense, had expressed an interest in the fifth generation F-35. The outcome, has under US advice, been the upgrade and extension of the existing F-16 fleet[1009]. In the first phase of this development under the Phoenix Rising programme, Taiwan opted to upgrade 64 of its existing 1990s F-16 fleet[1010]. Designated the F-16V, the change would between 2019 and 2023 offer improved radars, a new mission computer and upgraded electronic warfare abilities[1011].

Following this, Taiwan then agreed with President Obama in 2019 that it would procure 70 new built F-16C/D variants[1012]. With the delivery of these expected to be sped up in the face of increasing PRC military intimidation, it is now expected that Taiwan will by 2026 operate over 200 aircraft making it the largest F-16 fleet in Asia[1013]. Though differing in ages and variants, these F-16s will allow Taiwan to retire its ageing Mirages. Also operating alongside the continuing 120 IDFs, Taiwan will maintain a substantial number of proven fourth-generation fighters.

If discussed in the context of the ODC asymmetric approach to countering the PRC, this conventional air capability may, despite its size, seem increasingly irrelevant. This is because under ODC Taiwan's fighters would seek to deny PRC aircraft from entering its airspace as part of an integrated air defence. Working alongside the Patriot Advanced Capability 3 (PAC-3) and Tian Kung-2 surface to air missiles, fighters arguably become the least important element. Furthermore, with assessments indicating that few Taiwanese fighters would

[1009] For detail on the Taiwanese interest to procure F-35, see:
F. Gady, "Taiwan Wants the F-35 Stealth Fighter", *The Diplomat,* (2018).

[1010] For an overview of Project Rising Phoenix and the Taiwanese upgrade to the F-16V, see:
M. Yeo, "Taiwan Commissions First Upgraded F-16 Fighter Wing", *Defence News*, 19 November 2021.

[1011] For detail on the F-16V, see:
Lockheed-Martin, "Meet F-16v: The Most Technologically Advanced 4th Generation Fighter in the World", https://www.lockheedmartin.com/en-us/news/features/2016/meet-the-f-16v--the-most-technologically-advanced-4th-generation.html#:~:text=The%20F%2D16V%20configuration%20includes,Generation%20multi%2Drole%20fighter%20aircraft.

[1012] For a summary of the Taiwanese decision to upgrade its fleet to the F-16V, see:
Writer, "Taiwan Gives up on F-35, Turns to F-16v Option".

[1013] For reporting on the sale of the F-16C/D to Taiwan, see:
P. Stewart, "Exclusive: U.S. Seeks Way to Speed Delivery of New Fighter Jets to Taiwan", *Reuters*, 20 January 2022.

survive the PRC's initial bombardment of its airfields, this limited role for manned aircraft is marginalised even further[1014].

However, taken in the context of the expected replacement of ODC with plans to deter the PRC through missile strikes and direct combat, the size and capability of Taiwanese air power regains its vital importance. In this circumstance, one must turn to consider whether Taiwan's fleet of over 300 fourth-generation fighters are, if not quantitatively on par with the PRC, at least a qualitative match.

In answering this there is no doubt that Taiwan's planned fleet is a vast improvement on its legacy F-5, Mirage and early F-16 variants. However, despite these advances, it falls significantly short of the PRC's fifth-generation aircraft such as the J-20 which, despite themselves falling short of the F-35 performance, remain capable enough to outperform the newer F-16 variants[1015]. Adding to this it is also noted that US assessments of the PRC's capabilities indicate that it could now 'dissuade, deter, or…defeat third-party intervention during a large-scale, theatre campaign'[1016]. With this indicating that the PRC may be able to keep US assistance from reaching Taiwan in the event of a crisis, the mismatch between aircraft such as the F-16 which will be relied on to protect Taiwanese airspace and the J-20 designed to dominate it becomes starker.

This paints a troubling picture for Taiwan, which under its new plans is increasingly reliant on a credible air power capability to assure its fiercely held independence. However, whilst this cannot be denied, what is equally true is that with approximately 320 fighter aircraft at its disposal Taiwan operates a larger fleet than most other countries including the supposed Great Powers of the UK and France. Furthermore, in a period in which fifth generational air power is viewed by the Great Powers, including the PRC, as the air domain's panacea,

[1014] For this assessment of the marginalised value of Taiwanese fighter aircraft under OCD, see:
D. Axe, "Taiwan Might Experience Buyers Remorse over the F-16 Fighter", *The National Interest,* (2022).
Thompson, "Hope on the Horizon: Tawian's Radical New Defense ".

[1015] For a summary of the F-16V 'vs' the J-20, see:
Editorial, "F-16v Still Taiwan's Greatest Hope When Dealing with China's "Strongest Dragon" J-20", *Defence View,* (2022).

[1016] US, "Military and Security Developments Involving the People's Republic of China 2020", ed. US Department of Defense (2020), ix.

Taiwan's development of a relatively large fourth-generation fleet adds an additional dimension.

In this context, it becomes relevant to ask whether in a contested cyber domain platforms that employ, but are not as reliant on, digital capabilities may offer an operational edge. Furthermore, if they do offer this edge, it must also be asked whether in a Taiwan-PRC crisis they may be decisive? To address this, it is intuitive to finally turn to consider the cyber vulnerabilities of Taiwanese air power. Specifically, it is necessary to explore whether this island state's significant number of fourth-generation fighters might avoid cyber vulnerabilities which challenge fifth-generation fleets and, through their mass, maintain a necessary level of operational effectiveness to hold a PRC attack until US support arrives.

Cyber Vulnerabilities of Taiwanese Air Power

In exploring this question, the first point of discussion must be whether Taiwan's decision to focus on a large fleet of fourth-generation fighters rather than a smaller number of exquisite fifth-generation alternatives makes its air power less exposed to cyber vulnerabilities. If true, this offers a potential counter to the increasingly prevalent view within super, great, and other regional powers that fifth-generation aircraft represent a panacea in today's digitally enabled world. Specifically, the conclusion could be that the fourth-generation F-16 offers states of Taiwan's size and resource a high level of combat capability at a price that allows mass without the increasing cyber vulnerabilities experienced by complex platforms.

From one perspective the assumption that the F-16 and other aircraft of its era should be less cyber vulnerable has a logical foundation. In operation since the 1970s, the F-16 has been developed iteratively. Though recent versions such as the F-16V sold to Taiwan are a world apart from the low-cost, lightweight fighter the US commissioned over four decades ago, their slow development and integration of tried and tested technologies allowed each enhancement to be fully considered, tested, and assured[1017]. Offering a contrast to fifth-generation aircraft such as the F-35 which being at the cutting edge of technology have suffered repeated unseen issues, such iterative evolution should provide assurance that the F-16 is 'cyber hardened'.

Such claims are supported by Lockheed-Martin, the current manufacturer of the F-16. In open-source material on the aircraft produced by the company the platform is claimed to have been subject to extensive testing and analysis at every stage of upgrade. This has, according to Lockheed-Martin, extended the 'limits of the venerable F-16…[so that it will] continue to play a crucial role in international security for years to come'[1018]. If this argument is to be accepted, it could be concluded that Taiwan's large fleet of F-16Vs will be sufficiently resistant to cyber attack to operate effectively in a contested cyber environment. Furthermore, with a level of combat capability that allows them to challenge newer PRC variants, the F-16 will effectively form the backbone of the island's deterrence and holding strategies.

Despite this logic the USAF has itself acknowledged that the F-16 is not as cyber secure as might be expected. A position exposed in its Cyber Resilience Groups' instigation of a 2016 programme to improve the cyber security of its legacy systems, the USAF confirmed that it aims to work with operators, engineers, and contractors to address long standing concerns[1019]. Citing the F-16 as a key example of the need for this programme, General Ellen Pawlikowski, Commander of the USAF Materiel Command, commented that testing of its upgraded digital systems has, like many other legacy platforms, identified that it exhibits 'cyber threat surfaces all over the place'[1020].

Exploring how the F-16 could, despite Lockheed-Martin's assurances, experience so many cyber threat surfaces, it is instructive to reflect on cyber

[1017] For an overview of the development of the F-16, see:
K. Mizokami, "The F-16v, the Newest Version of the Iconic Fighter, Takes Flight", *Popular Mechanics,* (2015).

[1018] Lockheed-Martin, "Meet F-16v: The Most Technologically Advanced 4th Generation Fighter in the World".

[1019] W. Skowronski, "Vulnerability in Cyberspace", *Air Force Magazine*, December 2016.

[1020] For Pawlikowski's quote, see:
S.D. Carberry, "Air Force Scrambles to Harden Weapons Systems", *FCW*, 21 September 2016.

challenges within the wider aviation industry. Though to the casual observer aviation in all its forms can appear cutting-edge, behind the scenes the soft and hardware modern aircraft rely on is often based on dated technology[1021]. For many of these underlying legacy digital technologies, including some of those introduced to the F-16, cyber threats were not of primary concern in their design. This is because though these were often vital to operational delivery, the digital systems were routinely stand-alone allowing no logical routes by which an attacker could compromise them. However, with the expansion of IP connectivity across all industries including aviation there has been a drive to increase effectiveness and efficiency through interconnectivity. With such advancements both within platforms, between platforms and from air to ground support systems often introduced without considering second order cyber resilience effects, new vulnerabilities can be inadvertently introduced[1022].

Considered in more detail, the concern is not the creation of new cyber vulnerabilities. Rather, it is the emergence of new ways to access and exploit existing vulnerabilities that were previously thought uncompromisable without a physical connection. An example of this was identified in 2017 by the US DHS. Using commercially available equipment the DHS established a presence on the systems of a Boeing 757 commercial airliner through its RF communications[1023]. Achieved without a physical connection or insider assistance, the exploited vulnerabilities could, if achieved by a malicious actor, have endangered the aircraft. Whilst one might hope that such vulnerabilities cannot be found on military aircraft, Pawlikowski's comments in 2016 show that platforms such as the F-16 are equally at risk of legacy systems creating unseen cyber vulnerabilities[1024].

[1021] J. Bailey, "Airlines Need to Embrace It System Modernization: Here's Why", *Simple Flying* (2021).

[1022] C. Nobles, *Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications* (Pennsylvania: IGI Global 2019), 262.

[1023] For detail on the Boeing 757 example, see:

E. Urkandu, Ben-Farah, M., Hindy, H. , "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends", *Information System Frontiers*, no. 13 (2022).

Biesecker, "Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, Dhs Says".

[1024] For further depth on issues relating to legacy systems in aviation including both platforms and ground support systems, see:

US, "Faa Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to Nextgen", ed. Goverment Accountability Office (2015).

Focusing in on the F-16, the platform is acknowledged as having a plethora of digitally enabled 'mission data, sensors, missiles, intelligence information, precision guidance technology, data links and weapons targeting systems' which were once standalone[1025]. However, through the platform's evolution they have been increasingly integrated within the platform itself and through datalinks with both other airborne platforms and ground systems. Discussed by Pawlikowski at the 2016 Air Force Association Air Warfare Symposium, she outlined how this development has created distinct and exploitable areas of cyber vulnerability which place the F-16 at risk[1026]. Whilst in the same announcement she confirmed that resolving these were central to a USAF 'cyber campaign plan', the reality for those operating the F-16 is undiminished[1027]. Specifically, for states including Taiwan there is a credible concern that the apparently 'cyber hardened' F-16 is vulnerable to cyber attack from active persistent threat actors such as the PRC.

To illustrate the depth of Taiwan's cyber concerns with the fighter that it is now reliant on, it is informative to explore some of the areas identified by Pawlikowski. Beginning with mission planning, Pawlikowski noted how the USAF had recognised that the F-16 was dependent on mission planning conducted on secure digital systems. Though themselves protected from digital incursion, exercises conducted by the US have from as early as 1997 proven that such systems are prone to cyber compromise. Taking Joint Exercise Eligible Receiver 97 as an example, US NSA conducted penetration testing confirmed how systems like those used for F-16 mission planning could be compromised using commercially available equipment. Through these tests it was proved that such activities could achieve the exfiltration of information or the degradation of system performance[1028]. If such activity was directed against the Taiwanese F-16s mission planning systems, there is a potential that the PRC could either compromise operational planning and pre-empt tactics or degrade

[1025] C. Osborne, "Air Force: An F-16 Could Be Vulnerable to Cyber Attack", *Defence Systems* 18 October 2016.

[1026] For a summary of the 7 lines of attack, see:
K. Osborn, "U.S. Air Force: F-16s and Other Critical Weapons May Be Vulnerable to Cyber Attack", *The National Interest,* (2016).

[1027] S. Nicholas, "Gen. Ellen Pawlikowski: Cyber Resiliency Steering Group Unveils Air Force Cyber Campaign Plan", *Executive Gov* 23 September 2016.

[1028] For the full Exercise Eligible Receiver 97 report released as part of the US FoI Act, see:
US, "Eligible Receiver 97", ed. Department of Defense (1997).

the effectiveness of a Taiwanese response. In either circumstance, the impact on Taiwan's ability to hold a PRC advance until US assistance might arrive would be materially undermined.

With the example of compromise taken from 1997, it might be argued that such vulnerabilities should have been mitigated. However, reporting over the last 2 decades shows how the issue remains extant. For example, a 2019 US Cybersecurity Advisory note warned that the Russian GRU had conducted successful attacks against not only private sector but government and military networks[1029]. With US military systems including the Marine Corp Intranet (MCI) also compromised in 2013, and the PRC known to have a strong track record in targeting its adversaries' systems, a strong potential emerges of the Taiwanese F-16 mission planning systems being targeted and compromised[1030].

Developing this focus on Taiwan, the potential cyber issues become increasingly stark. With reporting in 2018 suggesting that Taiwan's military networks had been subject to over 200 million cyber attacks originating from the PRC in a single year, it is evident that there is credible PRC intent to compromise its systems and disrupt operations[1031]. Responding to this challenge in 2017, Taiwan formally established the world's first independent military cyber command in the form of the Information, Communication and Electronic Force (ICEF) Command. Becoming in practice Taiwan's 'fourth service', ICEF consolidated cyber and electronic-warfare elements that already existed in its wider armed forces[1032]. Pushing Taiwan to be recognised by the Australian Strategic Policy Institute (ASPI) in 2018 as the ninth most mature cyber power in the Asia-Pacific, there is no doubt that Taiwan recognises the threat[1033].

Notwithstanding this focus and associated advances, the Taiwanese military continue to face 'a myriad of cybersecurity challenges' and a PRC focused on

[1029] CISA NSA, FBI and NCSC, "Russian Gru Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments", ed. Cybersecurity Advisory Note (2021).

[1030] For reporting on the MCI compromise, see:
N. Norton, "The U.S. Navy's Evolving Cyber/Cybersecurity Story", *The Cyber Defense Review,* 1, no. 1 (2916).

[1031] S. Yang, "200 Million Cyber Attacks Hit Taiwan's Military Networks in 2017", *Taiwan Times*, 28 May 2018.

[1032] "Chinese Hacking against Taiwan: A Blessing for the United States?", *The Diplomat,* (2018).

[1033] F. Hanson, "Cyber Maturity in the Asia Pacific Region 2017", (Australian Strategic Policy Institute 2018), 11.

undermining its air power[1034]. Illustrated by the 200 million yearly cyber attacks and the huge volume of PRC incursions into Taiwanese airspace, there is little doubt that at a strategic level cyber and air power have been combined by the PLA[1035]. When overlaid with Pawlikowski's public warning that the F-16 mission planning systems could be compromised, it becomes likely that this specific vulnerability will have become an area of focus for the PRC. Given this, Taiwan should be concerned that its F-16 fleet may through cyber compromise be prevented from delivering the essential air deterrence they were procured to provide.

In a second area of F-16 cyber vulnerability, Pawlikowski expands the discussion of legacy issues to consider cyber vulnerabilities associated with technology acquisition. Recognising in this that the F-16 has been subject to 40-plus years of piecemeal upgrades, she returns to the theme of how a previously secure platform may have been made insecure through the introduction of new developments or capabilities[1036]. However, moving away from the issue of IP connectivity Pawlikowski, in this context, focuses on how new F-16 components could be compromised by hostile actors whilst in development or the supply chain. When considered in the context of the Taiwanese Rising Phoenix programme which has made the island dependent on the F-16V, this concern emerges as a potential that its upgraded aircraft may have become cyber vulnerable even before they reached the island.

This topic was, in broad terms, explored by Raymond O'Toole in his 2021 testimony to the US Senate Armed Service Committee. In this he highlighted that the US Office of the Director, Operational Test and Evaluation (DOT&E) had assessed in 2020 that due to supply chain cyber attack 'virtually none' of the military programmes it had reviewed were 'survivable against relevant cyber

[1034] For the quote, see:
C.D. Pryor, "Taiwan's Cybersecurity Landscape and Opportunities for Regional Partnership", *Center for Strategic and International Studies (CSIS),* (2018).

[1035] For reporting on PRC incursions into Taiwanese air space including 30 in a single day in May 2022, see:
Z. Jalil, "China Sends 30 Warplanes into Taiwan Air Defence Zone", *BBC News* 31 May 2022.

[1036] For this summary of the 'second line of attack', see:
Osborn, "U.S. Air Force: F-16s and Other Critical Weapons May Be Vulnerable to Cyber Attack".

threats'[1037]. Of note, this statement directly built on conclusions drawn in 2013 by the US DoD Science Board. In these, it was concluded that military aviation supply chain issues including the introduction of counterfeit parts may have created operational vulnerabilities on complex digital systems'[1038].

With such issues extrapolated out by the DoD Science Board reported to lead to potentially malicious examples of corrupted data and weapons failure, it becomes evident how a persistent hostile actor such as the PRC could undermine Taiwan's F-16 fleet through cyber means. Furthermore, the issue also illustrates how even with Taiwan's rise to the ninth most mature cyber power in the Asia-Pacific, its reliance on the US for military support and equipment means that many of its cyber vulnerabilities are outside its control[1039]. Based on this, the founding of its deterrence strategy on the large F-16 fleet becomes increasingly problematic when placed in the context of a large, aggressive, and cyber capable PRC investing resources at every level to undermine Taiwanese air power.

Looking beyond Pawlikowski's attack-vectors and the F-16 itself, other cyber vulnerabilities should also concern Taiwanese air power. The first of these is a credible malicious insider vulnerability within the Taiwanese military. Highlighted in media reporting emerging in December 2021, official Taiwanese documents allege that the PRC intelligence services have successfully recruited Taiwanese Military Officers[1040]. Focusing on the specific case of a supposed Hong Kong businessman, Xie Xizhang, the documents suggested that the PRC through this agent had penetrated the Taiwanese military. These included according to reporting those in senior command positions and a senior Military Police Officer within the Taiwanese Presidents protection detail[1041].

Though the reports make neither mention of cyber compromise or air power, the sheer scale of the PRC effort in Taiwan, the PRC's known focus on cyber

[1037] R. O'Toole, "Hearing to Receive Testimony on Defense Aquisition Prograems and Aquisition Reform ", ed. United States Senate Committee on Armed Services (2021).
[1038] US, "Resilient Military Systems and the Advanced Cyber Threat", ed. Department of Defense Defense Science Board (2013).
[1039] For further discussion on this US cyber supply chain vulnerability and its impact on military aviation capabilities, see: G. Hadley, "Hacking the Supply Chain ", *Air Force Magazine*, 3 December 2021.
[1040] R. Wood, "Chinese Spy Ring 'Penetrating Taiwan Armed Forces'", *9 News* 22 December 2021.
[1041] Y. Lee, Lague, D. , "T-Day: The Battle for Taiwan", *Reuters* 20 December 2021.

vulnerabilities and the importance of air power to the deterrence strategy makes the issue a real concern. For example, reporting in 2017 confirmed that Taiwan's national security authorities estimated there to be 5,000 PRC spies in Taiwan with 80 percent of those focused on the military[1042]. With analysis of PRC intelligence techniques suggesting that it is increasingly 'integrating human and technical means of collection to boost effectiveness' there is a credible possibility that these spies are targeting digital systems[1043]. Furthermore, with intelligence on the capability of Taiwanese air power a likely intelligence priority for the PRC, it is probable that many of these attempts to compromise systems are directed against air power related areas. Given this, the malicious insider vulnerability though oblique in terms of cyber must be considered as a credible vulnerability which may impact Taiwan's air power capability.

Turning to a further indirect cyber vulnerability, the issue of infrastructure must be considered. As an island nation without a carrier capability, Taiwan is restricted to mounting air operations from a relatively small number of land-based airfields. With air power uniquely infrastructure reliant when compared to land or maritime operations, and the infrastructure which supports modern air power reliant on integrated and interconnected systems, the targets for the PRC to focus cyber attacks on to disrupt air operations become relatively well defined[1044]. With such cyber attacks likely to include airfield lighting, fuels, and power systems, it becomes probable that the PRC is actively searching for infrastructure vulnerabilities within its intent to disrupt Taiwanese air power.

Exploring this further, the Taiwanese Air Force does, considering its size, have the advantage of operating from a reasonably large variety of 13 air bases. These are spread across the main island and other smaller islands including Penghu and Taiping. However, except for 3 military airfields these are all co-located within civilian airfields[1045]. Given this, Taiwanese air power becomes largely dependent on the operations of its civilian host airfields.

[1042] C. Li-hau, "5,000 Chinese Spies in Taiwan", *Taipei Times*, 13 March 2017.
[1043] P. Mattis, "A Guide to Chinese Intelligence Operations ", *War on the Rocks* (2015).
[1044] UK, "Joint Tactics, Techniques and Procedures 4-05: Operational Infrastructure", 1-4.
[1045] Solely military Taiwanese airfields are Chhihaang, Chiashan and Ching Chuan Air Bases.
I Easton, "Taiwan, Asia's Secret Air Power", *The Diplomat,* (2014).

Though little is published on the cyber security provision for these civilian airfields, widespread analysis from other countries underlines how aviation's increasing reliance on the IIoT and CPS for airfield infrastructure are creating cyber vulnerabilities[1046]. Of note, analysis in this area focuses on the embedded SCADA systems which control virtually all industrial processes including fuels and power to airfields, and how these systems routinely use the internet as a bearer for communications[1047]. With these factors viewed as creating numerous cyber vulnerabilities for airfield infrastructure, and the PRC undoubtedly aware of them, it is logical to assess that Taiwan's use of civilian airfields will be understood and their vulnerabilities mapped. Through this, it can be further judged that in the event of a Taiwan-PRC crisis cyber attacks against airfield infrastructure will be employed to undermine the effectiveness of the air power response.

With academics including Libicki highlighting that even an organisation as large as the US DoD only controls a relatively small amount of their digital infrastructure, it is further possible to judge that such vulnerabilities will in part also impact Taiwan's 3 military airbases[1048]. Further underpinned by reports from India in 2020 which indicate that the PRC has successfully targeted its adversary's critical infrastructure, this potential left-of-launch cyber vulnerability against Taiwanese air power becomes increasingly credible and concerning[1049].

Taken collectively, the above analysis of direct and indirect cyber vulnerabilities associated with Taiwanese air power paints a concerning picture. Faced with a credible adversary in the form of the PRC which is driven to achieve reunification with the island, Taiwan has become focused on a relatively large fleet of fourth-

[1046] For an example of research in this area, see:
Masood and Sonntag, "Industry 4.0: Adoption Challenges and Benefits for Smes".

[1047] For analysis in this area, see.
Ervural and Ervural, "Overview of Cyber Security in the Industry 4.0 Era," 272.

[1048] Libicki, "Cyberspace Is Not a Warfighting Domain", 326.

[1049] Following border disputes between PRC and India in 2020 media reports indicated that the PRC used trojan horse malware to attack the Indian Maharashtra State Electricity Board (MSEB). Though a tangential example, it shows how the PRC has developed and used the ability to successfully target an adversary's key infrastructure. For reporting on and analysis of this event, see:
D. Sanger, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out", *The New York Times* 28 February 2021. Staff-Writer, "India-China Dispute: The Border Row Explained", *BBC News Online*, 25 January 2021.
"Mumbai Power Outage in October May Have Been Result of 'Cyber Sabotage'", *The Wire* 2 March 2021.

generation aircraft to underpin the deterrence strategy. Despite logic and manufacturer assurances that this air power should be less vulnerable to cyber attack than fifth-generation alternatives, it has been shown that an extensive array of attack-surfaces may be used to compromise the capability even before flight is achieved. In this context, cyber vulnerabilities have therefore introduced a credible potential of undermining or removing Taiwan's principle means of deterrence and defence even before a kinetic conflict with the PRC begins.

Conclusions on Taiwanese Air Power Cyber Vulnerabilities

Having justified the inclusion of this Taiwanese case study through its position as a Western aligned state, it was identified as one whose role has generated a geopolitical importance more significant than its size suggests. Examining whether Taiwan holds the military power to preserve the independence upon which this role rests, it was identified how despite shifting reforms air power remains central to the islands defence. With this responsibility now resting on a significant procurement of enhanced fourth-generation F-16 fighters, the discussion explored how the platforms may be susceptible to cyber vulnerabilities.

Considering the discussion of these vulnerabilities, alongside an exploration of how the PRC could use cyber means to deny Western access to the region, an existential threat emerges. Given this stark reality, Taiwan's cyber concerns emerge as having the most profound strategic impact of all the case studies discussed in this Chapter. With parallels able to be drawn to other similarly sized states with aggressive neighbours, a necessity is identified to invigorate their mitigation of cyber vulnerabilities to air power. If this is not achieved, these smaller regional states may in the short-term face a realist existential threat which eclipses the role-based concerns of great and superpower states.

Conclusion

To open this part of the thesis' discussion on Western air power's cyber risk, this Chapter examined the cyber vulnerabilities of air power through three representative lenses: the US as a superpower, the UK as a great power and Taiwan as a regional power. Adopting a common approach to each, their development towards contemporary roles were initially discussed before military and air power capabilities were examined. Using this process for each, a final examination of their air power cyber vulnerabilities was offered in the context of history, contemporary position, and military power.

Beginning with the superpower of the US, the section charted its development through bipolarity and unipolarity before looking towards an uncertain future. Combined with an exploration of US strategic culture, its contemporary conceptualisation as an 'exceptional' power was identified. Developing the discussion in terms of whether the US has the military power to achieve its 'exceptional' role, it was noted that despite its significant capabilities the scale of its ambition is increasingly uncertain in an era of great power competition. Placing this in the context of air power, it was noted how the US has become reliant on an advanced but reduced number of air capabilities. This may, it was concluded, lead the US to struggle to effectively balance the strategic scales in its favour.

With this understanding in place, this US section finally explored its air power's cyber vulnerabilities. Delivered through three distinct discussions, the direct threat to US air power with specific reference to the F-35 was initially explored before left-of-launch and cyber espionage were discussed. Taken collectively, these illustrated a concerning picture of a superpower whose air power on which it relies might be undermined by multiple cyber vulnerabilities. As a result, it was concluded that the US will struggle to maintain its self-conceived exceptional global role unless the 'Achilles heel' of cyber can be effectively mitigated.

Turning next to the great power of the UK, the section began by charting the UK's gradual decline from superpower status and how this legacy has created a constructivist 'Global Britain' role. Viewed in a contemporary sense, it was noted how this role has been increasingly challenged by events including BREXIT, a strained Anglo-US relationship and COVID. Collectively, the impact was identified as a residual great power struggling to maintain its global aspirations. Taken in this context, the section's exploration of UK military power found that, despite struggling to meet commitments such as NATO's spending targets, it still strives to balance relative decline with the military lever. To achieve this, the discussion of UK air power showed how this is being manifested in a reliance on a small number of advanced platforms which will struggle to assure its global residual-great power role.

Developing these assertions into UK air power's cyber vulnerabilities, the advanced F-35, an increased use of UCAV platforms and its limited air power infrastructure were focused on. Taken together, it was shown how the UK which is facing relative decline and a desire to maintain its global role had invested in a form of low mass high technology that is susceptible to cyber vulnerabilities. As a result, it was concluded that the UK must view its cyber vulnerabilities not as technical or military issues, but a national concern which, if not resolved, may prevent the maintenance of its residual great power role.

Finally, considering the regional power of Taiwan, its inclusion in the discussion was initially justified. Shown to offer an insightful regionally focused case study, the section initially charted the island's development towards its contemporary position. Shown to have a distinct identity of fierce independence, Taiwan emerged as an island whose role had generated a geopolitical importance more significant than its size suggests. With this established, it was next considered whether Taiwan has the military power to secure its independence. Explored through Taiwan's developing strategies, it was shown how with the US as a constant 'golden thread', the island has maintained a relatively stable focus on deterrence. However, considering recent statements it was also shown how Taiwan is moving away from holding the PRC to threatening retaliation through missile strikes and direct combat. With air power central to this, the discussion turned to consider whether it has the air capability to back the intent. In this, it was shown how Taiwan aims to achieve its plans by investing in a large F-16V fleet.

With this baseline established, the section next considered whether cyber vulnerabilities to air power may affect the strategic calculus. Focusing initially on the F-16V before exploring the malicious insider threat and infrastructure, it was established how despite the argument that less cutting-edge capabilities will be less vulnerable to cyber, numerous concerns still exist. Including the identification of new digital pathways into legacy capabilities, it was ultimately found that an adversary such as the PRC could undermine Taiwanese air power through cyber. Taken alongside other factors, this was concluded as having the possibility of shifting the PRC's strategic calculus. Therefore, cyber vulnerabilities emerge as a significant concern for a state which is reliant on air power to assure its survival.

Reviewed in its totality, this Chapter has shown two key and consistent themes. Firstly, exquisite fifth-generation platforms by deign of their reliance on digital technologies are most exposed to the impact of cyber vulnerabilities. However, though correct, all platforms in this digitally connected world whether iteratively enhanced fourth-generation technologies or unmanned are also vulnerable. Therefore, all air forces whatever they operate must actively identify and mitigate against cyber vulnerabilities to remain operationally viable.

Secondly, though air platforms themselves are naturally the focus of such discussions, it may be indirect cyber vulnerabilities that are most exposed to hostile compromise. Largely found in the broad scope of left-of-launch concerns and ranging from malicious insiders, through ground support systems to infrastructure, it is this area which must be addressed through a holistic approach to the issue.

Taken collectively, the reality for all air forces whether that of a super, great or regional power is that whilst the kinetic threats remain real and means to harden assets from attack necessary, it is in the cyber domain where conflict may be won or lost. With this potentially extending years ahead of a bullet being fired through issues including supply chain vulnerabilities, there is a pressing requirement for a far-reaching approach to cyber security if a state's air power is to remain viable.

Placing this into the context of specific challenges facing super, great and regional powers, a level of concern is identified that becomes inverse to a state's size. Specifically, whilst all forms of air power are subject to cyber vulnerabilities the size and diversity of the US as a superpower means that impacts can be mitigated. This issue increases, however, for great powers such as the UK. Reliant on a small number of advanced platforms with limited variety, the loss of one fleet through the exploitation of a cyber vulnerability may materially impact maintenance of its role. Though concerning, the issue reaches a pinnacle for regional powers faced with existential threats. In this context cyber vulnerabilities, if exploited, may remove a key air power deterrence. Likely to shift an adversary's strategic calculus, the result may be a conflict of existential proportions.

In conclusion, cyber vulnerabilities are therefore of concern for all states but become increasingly important the less resilient they are to the potential impacts. Though deeply concerning, to judge the full cyber risk, the intent and capability of the threat actor's focused on exploiting vulnerabilities must be known. It is this factor that will be addressed in Chapter 7.

Chapter 8: The Cyber Threat to Western Air Power

Introduction

This Chapter will build on the previous discussion of cyber vulnerabilities by exploring the potential cyber threats to Western air power. This will be achieved through an exploration of the representative examples of the PRC as a superpower in waiting, Russia as a great power pushing to maintain global relevancy and Iran as a regional power seeking to assure influence. Adopting common themes throughout, the Chapter will, for each of the respective states, consider its relationship with the West before delving into the nature of the cyber threat they pose and their supporting cyber capabilities. Through this, conclusions will be drawn on the level of the cyber threat each state poses to Western air power.

Exploring these initial conclusions in a closing section it will be noted that a cohesive but complex picture is presented. In terms of its cohesiveness, all 3 examples will be shown to demonstrate a parallel and credible cyber threat to Western air power. Concurrently, however, it will also be noted that each threat exhibits distinct characteristics with the PRC’s grey zone methods long term in nature, the Russian hybrid approach focused on achieving immediate gain and Iran’s capabilities designed to achieve operational level regional gains.

Finally reflecting on this cohesive but complex picture, the Chapter will close by asserting that the cyber threat to Western air power is backed by a range of credible intents to achieve strategic advantage through cyber means. Further underpinned by varying but uniformly credible cyber capabilities there is, it will be concluded, little doubt that the West faces a concerning cyber threat to its keystone air power capabilities.

People's Republic of China (PRC)

Introduction to the PRC Cyber Threat to Western Air Power

To begin this discussion of cyber threats to Western air power, this initial section will focus on the PRC. Opening with an overview of Western-Sion relations, it will be noted that since the 2000s fundamental differences between the West and the PRC have created entrenched positions. For the PRC this is defined by a perception of the West attempting to deny its rightful emergence, whereas for the West it is focused on a perception of an aggressive, expansionist PRC set on ignoring the rightful sovereignty of others. With this likely to 'shape geopolitics for decades', the discussion will identify the key question as being whether the PRC's cyber capabilities may be decisive in this competition and, if so, how they may threaten the strategic viability of Western air power[1050].

To address this, the section will consider in turn the nature of the PRC cyber threat and whether this is backed by credible capabilities. Drawing the discussion to a close, it will finally be argued that cyber will play a key role in both the PRC's path to, and conduct of, any potential Sino-Western conflict. With this including the PRC's disruption of Western air power, the section will assess that the PRC's use of cyber offers a blueprint for how a rising power can achieve its goals through cyber means without necessarily resorting to armed conflict.

Sino-Western Relations

After its inward-looking Cultural Revolution ended in 1976 the PRC would, in the last quarter of the 20th century, achieve unparalleled development. Transforming from low-cost, low skill manufacturing to a global leader in advanced technologies, its economy would double in size every 8 years placing it in the top 10 of global economies by 2000[1051]. Accompanied by a diplomatic shift in the

[1050] For the quote, see:
B. Jones, interview by Brookings Institute, 2021.

[1051] US, "China's Economic Rise: History, Trends, Challenges, and Implications for the United States", ed. Congressional Research Service (2019), 4.
N.R. Lardy, "Issues in China's Wto Accession ", *Brooking Institute,* (2001).

1990s, the PRC also engaged in bilateral relations, international agreements, and multilateral organisations. Welcomed by the West as a potential ally, it was rewarded by the normalisation of trade relations with the US in 2000, membership of the World Trade Organisation (WTO) in 2001 and unprecedented levels of direct foreign investment[1052].

Though the PRC's transformation to a rising great power with legitimate superpower aspirations appeared harmonious, fracture lines in Sino-Western relations soon appeared. Driven by fundamental differences in governance, economic practices, and human rights, it was clear by the 2000s that the PRC's strategic focus was not to fall in line with Western norms but remould the international system to meet its strategic intent[1053].

From the PRC's perspective, this was legitimate[1054]. Explained in its 2015 Defence Strategy, the PRC argued that with 'profound changes taking place in the international situation' the balance of power, global governance structures and the importance of the Asia-Pacific geostrategic landscape placed it, not the West, at the centre of geopolitics[1055]. Reinforced by its 2019 strategic White Paper on Defence, the PRC concluded that whilst it was peacefully embracing this shift, the West and its allies were refusing to accept the new reality. Citing unilateral US, NATO and EU defence and economic policies as creating Asia-Pacific security dilemmas, the PRC has interpreted Western actions as hegemonic, driven by power politics and a neo-interventionism intended to limit its rightful emergence as a global leader[1056].

[1052] For the development of US-Sino diplomatic relations, see:
Staff Writer, "Us Relations with China: 1949-2021", *Council on Foreign Relations,* (2021).
For membership of the WTO, see:
Lardy, "Issues in China's Wto Accession ".
For direct foreign investment, see:
US, "China's Economic Rise: History, Trends, Challenges, and Implications for the United States".
For depth on the PRC's development, see:
Editor, "How a Rising China Remade Global Politics ", *World Politics Review,* (2022).

[1053] T. Chhabra, Haas, R., "Global China: Domestic Politics and Foreign Policy", *Brooking Institute,* (2019).

[1054] M. Schuman, "What Happens When China Leads the World", *The Atlantic* (2020).

[1055] People's Republic of China, "China's Military Strategy of 2015", ed. The State Council Information Office of the People's Republic of China (2015).

[1056] Ibid., 2-6.

In response, the PRC’s 2019 Defense White Paper outlined how it would manage this perceived Western threat through four key objectives: safeguard its sovereignty against incursions, prevent foreign hegemony, expand spheres of influence in the Asia-Pacific, be capable of attacking if attacked, and, through the ‘Chinese way’, become an unparalleled power by 2049[1057]. Though objectively logical, in combination, especially when underlined by the ‘Chinese way’ which rejects Western defined norms of international behaviour, the West considered the PRC to not be legitimately growing but actively destabilising the international system[1058]. In evidencing this, the West and its allies routinely cite PRC actions in the Asia-Pacific region as those of an aggressive, expansionist state set on ignoring the rightful sovereignty of others.

A key example highlighted by the West and its allies to evidence this is the Senkaku islands in the East China Sea[1059]. Under Japanese sovereignty for over 120 years the PRC, recognising valuable natural resources, initially claimed historic land rights in the 1970s[1060]. Though Japanese-Sino talks to defuse tensions were held in the 2000s, a declaration by the PRC of an Exclusive Economic Zone (EEZ) in 2012 and Air Defence Identification Zone (ADIZ) in 2014, both of which encompassed the islands, stoked tension. Brought to a head by US President Obama in his 2014 statement that the islands were covered by the US-Japan Security Treaty, an impasse was set[1061]. Leading to high levels of PRC military aircraft activity over the islands, activity routinely met by Japanese fast jets, the area offered the West a case study of where the PRC’s perceived aggressive expansionism is destabilising the region[1062].

[1057] People's Republic of China, "White Paper: China’s National Defense in the New Era", ed. The State Council (2019), 7.

[1058] Ibid.

[1059] The islands are also referred to as Diaoyu by the PRC.

[1060] Staff Writer, "Tensions in the East China Sea", *Council on Foreign Relations,* (2022).

[1061] For Obama’s comments, see:
A. Panda, "Obama: Senkakus Covered under Us-Japan Security Treaty", *The Diplomat,* (2014).
For the Treaty, see:
Japan, "Treaty of Mutual Cooperation and Security between Japan and the United States of America ", ed. Japan Ministry of Foreign Affairs (1990).
For the PRC response, see:
Q. Gang, interview by J. McCurry, Branigan, T., 24 April 2014.

[1062] For Sino-Japanese air power tensions in the Senkaku islands, see:
Japan, "Statistics on Scrambles through the First Quarter of Fy2019", ed. Japan Ministry of Defence - Joint Staff Press Release (2019).
Staff Writer, "China-Japan Hotline Launched to Avoid Sea, Air Clashes", *South China Morning Post* 8 June 2018.

A second example is the South China Sea in which the PRC has built artificial islands and declared the 'Nine-Dash Line' to lay claim to the entire maritime area[1063]. Considered a flagrant breach of international law by the West, these activities are frequently cited as illustrating its expansionist activity[1064].

In exploring the PRC's motivations behind this perceived intent to destabilise, Western scholars offer numerous explanations. Though these range from a historic motivation to settle scores, through to a drive for natural resources and realist assertions of a growing power seeking to disrupt US hegemony, the outcome for the West remains the same[1065]. Specifically, viewing the PRC as a 'real danger' to the International Rules Base System (IRBS), the West has in the last 15 years consciously shifted its defence policies[1066]. Illustrated by the US's restoration of great power competition to the highest tier of defence priorities, and a broader diplomatic 'pivot to Asia', the Western intent to contain the PRC is clear[1067]. However, what remains unclear is the outcome when this unyielding Western position meets the PRC objective of becoming an unparalleled power by 2049[1068]. With Jones suggesting that this irreconcilable difference will walk the world into a strategic conflict that 'will shape geopolitics for decades', there is a requirement to consider how conflict may playout[1069]. For this thesis, the key question is whether the PRC's cyber capabilities would be decisive in such a conflict and, if so, how these may threaten the strategic viability of Western air power[1070].

[1063] For building of islands, see:
M. O'Hanlon, "China, the Grey Zone, and Contingency Planning at the Department of Defence and Beyond", *Brooking Institute,* (2019): 4; M. Tsirbas, "What Does the Nine-Dash Line Actually Mean?", *The Diplomat,* (2016).
The Nine-Dash line is a PRC marker which it uses to demark its maritime sovereignty. For depth, see:
J.A. Bader, "The U.S. And China's Nine-Dash Line: Ending the Ambiguity", *Brooking Institute,* (2014).

[1064] E. Freund, "Freedom of Navigation in the South China Sea: A Practical Guide", *Belfer Center,* (2017).

[1065] O'Hanlon, "China, the Grey Zone, and Contingency Planning at the Department of Defence and Beyond", 4.

[1066] Ibid.

[1067] For the shift in US defence priorities, see:
Ibid., 1.
For a summary of the 'pivot to Asia', see:
J. Milot-Poulin, Sarfati, R., Paquin, J., "The American Strategic Pivot in the Indo-Pacific ", *Policy,* 15 (2021).
"Territorial Disputes in the South China Sea - Global Conflict Tracker".

[1068] China, "White Paper: China's National Defense in the New Era", 7.

[1069] Jones, "Global China: Assessing China's Growing Role in the World."

[1070] O'Hanlon, "China, the Grey Zone, and Contingency Planning at the Department of Defence and Beyond", 1.

The Nature of the PRC Cyber Threat

The nature of the PRC cyber threat is most clearly articulated as being core to its pursuance of grey zone conflict. Though often used interchangeably with the term hybrid conflict, the two can be clearly demarcated. Firstly, whilst hybrid focuses on the tactical to operational levels, grey zone reaches into the strategic[1071]. Secondly, though hybrid employs capabilities ranging from conventional to non-conventional for a desired effect, grey zone focuses on their use below the threshold of kinetic conflict[1072]. Understood in this way, the PRC's multifaceted use of means to achieve political aims are most accurately defined as grey zone in nature[1073].

In exploring the nature of the PRC cyber threat within this, an intuitive starting point is the PLA strategy. Identifying cyber as core to its broader concept of Information Operations (IO), the PLA places the capability alongside electronic and psychological warfare as an integral element in achieving information superiority. Once realised, the PLA believes that through such information superiority a stronger foe can be countered, and political aims achieved, before conventional conflict is necessary[1074]. To achieve this aim, the PRC has expedited the development of its cyber forces with a focus on the collection of intelligence, the constraining of an adversary and, only when the grey zone has been exhausted, a force-multiplier for kinetic attacks[1075].

[1071] D. Carmont, Belo, D. , "War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare", *Canadian Global Affair Journal* (2018): 5.

[1072] S. Bachmann, Dowse, A., Gunneriusson, H., "Competition Short of War–How Russia's Hybrid and Grey-Zone Warfare Are a Blueprint for China's Global Power Ambitions", *Australian Journal of Defence and Strategic Studies,* 1, no. 1 (2019): 45.

[1073] Examples of such multifaceted approaches include the PRC's employment of the coast guard to coerce foreign fishing vessels, the creation of manmade islands and its Belt and Road Initiative (BRI).

For an example of Chinese Coast Guard activity, see:

J. Gomez, "China Coast Guard Uses Water Cannon against Philippine Boats", *ABC News*, 18 November 2021.

For a discussion of PRC manmade islands, see:

S. Pasandideh, "Do China's New Islands Allow It to Militarily Dominate the South China Sea?", *Asian Security* 17, no. 1 (2020).

For a summary of the BRI, see:

Y. Jie, Wallace, J., "What Is China's Belt and Road Initiative ", *Chatham House,* (2021).

[1074] US, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019", ed. US Department of Defense (2019), 64.

[1075] Ibid.

Aiming to fully integrate cyber by 2035, a key step forward for the PLA was its 2015 establishment of the Strategic Support Force (SSF). Delivering centralised control of all PLA non-conventional capabilities, the SSF will employ the advances to be achieved by 2035 to create and maintain the intended strategic initiative[1076]. In examining this intent, three key operational areas are highlighted.

In the first, the degradation of Western advantage through cyber espionage, the long-term visionary nature of the PRC cyber threat is made clear. Focused on enhancing its indigenous modernisation efforts to achieve strategic advantage against the West long before kinetic conflict is reached, recent technological advances show how successful the PRC has been[1077]. For example, the indigenous J-20 'Mighty Dragon' fighter has technologically 'closed the gap' on Western aircraft. However, when examined, striking similarities between the J-20 and the F-35 are identified. Including its sensor systems which look virtually identical to the F-35 Electro-Optical Targeting System (EOTS), such development led to strong suspicions that the PRC's impressive enhancements were not home generated but the result of theft of Western technologies.

This suspicion was not only proven in 2015 by the Snowdon leaks, but it was also confirmed that the theft had been achieved through cyber espionage. Specifically, the leaked documents showed how PRC state-sponsored hackers had stolen sensitive information on the F-35 from Lockheed-Martin systems in 2007[1078]. Laying bare the strategic advantages of cyber espionage which allowed the PRC to close the air power gap on the West and arguably shift the Asia-Pacific balance of power, the strategic impact of PRC cyber capabilities is illustrated[1079].

In a second area, the development of A2AD capabilities using in part cyber means again shows how the PRC is intent on preventing conflict before it occurs.

[1076] For depth on the SSF, see:
K. Pollpeter, M.S. Chase, and E. Heginbotham, "The Creation of the Pla Strategic Support Force and Its Implications for Chinese Military Space Operations", *RAND,* (2017).
[1077] US, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019", 130.
[1078] Applebaum, "Nsa Preps America for Future Battle".
[1079] Gady, "New Snowdon Documents Reveal Chinese Behind F-35 Hack".

In this it is noted that A2AD is criticised by some as an over emphasised term in relation to the Asia-Pacific[1080]. However, the PRC's effective development of A2AD capabilities is argued by many others as likely to soon be able to effectively 'shut down' Western military access to the region, including through air power, unless the West is willing to accept mass loss of platforms and casualties[1081]. Effectively preventing the West from engaging the PRC even before a conflict has begun, A2AD rebalances power in the Asia-Pacific[1082].

To achieve this, the PRC is not only focusing on conventional means such as the HQ-9 long range SAM system but is also employing cyber means via left-of-launch vectors[1083]. Unconventional in its approach, this cyber A2AD variant does not threaten adversaries kinetically but, by achieving 'cyberspace superiority', harnesses the ability to degrade an adversary's networks and system at will if they attempted to aggressively operate in the Asia-Pacific region. Given the reliance of Western capabilities on digital systems and networks, especially Western air power, even the credible threat of such a cyber capability could be decisive[1084]. In this way, the nature of the PRC grey zone cyber threat to prevent conflict is again clearly presented.

In a third area, counter-space, the PRC is again looking towards left-of-launch cyber to degrade an adversary's ability to act. Displaying both the intent and capability to employ cyber means in this way, the PRC has proven an ability to target space-based assets[1085]. If achieved in a crisis ahead of a conflict such

[1080] For criticism of the use of A2AD, see:
L. Simon, "Demystifying the A2ad Buzz", *War on the Rocks* (2017).

[1081] For a summary of A2AD and its importance, see:
S. Roblin, "Why China Has Went All-in on Chinese A2/Ad", *The National Interest,* (2021).
For the requirement for the West to accept mass casualties if it is to challenge PRC A2AD, see:
D. Mujumdar, "New Report Details Why a War between China and America Would Be Catastrophic", ibid. (2016).

[1082] D.C. Gompert, Cevallos, A., Garafola, C.L. , "War with China: Thinking the Untinkable ", *RAND* (2016).

[1083] For detail on conventional PRC anti-air A2AD, see:
N. Tri, "China's A2/Ad Challenge in the South China Sea: Securing the Air from the Ground", *The Diplomat,* (2017).
US, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019", 54.

[1084] "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019", 56.

[1085] Events which prove the PRC's development of effective cyber based counter-space capabilities include its alleged 2007 and 2008 cyber attacks on the US Geological Survey's Lundsat satellite and its alleged 2014 cyber attack on the US NOAA satellite. For depth on these events, see:
Harrison, Johnson, and Roberts, "Space Threat Assessment 2018", 13.

means would, as discussed in Part 2 of this thesis, disrupt Western military capabilities, especially air assets, to a point at which they are strategically unviable[1086]. In doing so, the PRC would achieve strategic advantage and its political aim before a kinetic exchange occurs[1087].

When the PRC's use of cyber means in espionage, A2AD and counter-space are taken collectively, the nature of the grey zone cyber threat to disrupt military capabilities including air power is evidenced. If successfully employed, or even credibly communicated, the PRC could effectively deter the West from considering a military challenge to the PRC in the Asia-Pacific. Opening the door for the PRC to engage in major expansionist activities it would, through cyber means, achieve its political intent of preventing foreign interference in its near abroad in the 'Chinese way' without a shot being fired.

PRC Cyber Capabilities

Though the intent to employ cyber in its pursuit of grey zone conflict in this 'Chinese Way' is clear, to be successful the PRC must hold the necessary cyber capabilities. Whilst the PRC itself recognises a technological delta with the West, one it publicly states it will remedy by 2049, it has nonetheless displayed an impressive depth of cyber capabilities that are already having strategic impact[1088].

Beginning with its most prolific source of cyber operations, cyber espionage, the PRC has in many ways already outstripped its adversaries. Though gains through this vector have directly manifested themselves in the military space, including air power, Western intelligence agencies assess that the PRC routinely achieves indirect military gains through the long-term targeting of political, business, and

Chen, "Opening Statement of Mr David D. Chen Independent Analyst: Hearing before the Us China Economic and Security Review", 75.
Perrotto, "China Key Suspect in Us Satellite Hacks."
For depth on the 2014 attack, see:
US, "Us China Economic and Security Review Commission: 2015 Report to Congress", 296.

[1086] For comment on the level of damage cyber attacks could achieve against space-based assets and the subsequent disruption to military capabilities, see:
Rajagopalan, "Electronic and Cyber Warfare in Outer Space", 1.

[1087] US, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019", 52.

[1088] Ibid., 31.

educational organisations[1089]. Acquiring sensitive military information via oblique routes, this cyber espionage has been identified as a key factor in the continued strategic shift in the Sino-Western balance of power[1090].

Tracked by the West, PRC state-sponsored cyber espionage was identified from the early 2000s. With reporting routinely linked to APT1, a hacking group also referred to by its military designators of 61398, its association with the PLA is well documented[1091]. Associated with a string of high-profile cyber espionage attacks, APT1 activities are reported to have included Operation Aurora in 2009. The exploitation of a zero-day vulnerability in the Microsoft Internet Explorer, APT1 gained access through this to numerous commercial networks[1092]. With this access including the source code repositories of defence contractor Northrop Grumman, and with Northrop Grumman being a key contributor to the F-35 programme, it is logical to assess that the access informed the development of the J-20[1093]. By doing so, this early example of PRC cyber espionage was undoubtedly pivotal in its intent to close the technology gap with the West and, by doing so, rebalance the strategic balance of power[1094].

Further reporting confirms the scale, discipline, and focused nature of PRC cyber espionage. Of note, these characteristics are personified by the PRC state-sponsored hacking group commonly known as Barium[1095]. Proven in 2017 to be behind a supply chain attack in which trojan horse backdoors were introduced into NetSarang, a popular South Korean remote management tool, Barium achieved extensive access to numerous organisations. With this same code found in a 2019 software update pushed by the Taiwanese based PC manufacturer Asus to over 57,000 customers over 5 months, an unrivalled pattern

[1089] US, "Cybersecurity Advisory - Chinese State-Sponsored Cyber Operations: Observed Ttps", ed. Cybersecurity and Infrastructure Security Agency (CISA) National Security Agency (NSA), Federal Bureau of Investiation (FBI) (2021).
[1090] "Cybersecurity Advisory - Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities ".
[1091] Mandiant, "Apt1 Threat Intelligence Report ", (2013).
[1092] B. Johnson, "Chinese Hackers Used Microsoft Browser to Launch Google Strike", *The Guardian* 15 January 2010.
[1093] J. Rosenberg, "Security in Embedded Systems " in *Rugged Embedded Systems* ed. A. Bose Vega, P. (Burlington: Morgan Kaufmann, 2017).
[1094] For Northrop Grumman's involvement in the F-35 programme, see:

B. McKinney, "Using Automation and Robotics in Advanced Aircraft Production", (Northrop Grumman, 2022).

[1095] Barium is also known to have operated under other names including Wicked Panda, ShadowHammer and ShadowPad. For detail on Barium and its associated names, see:

GoldSparrow, 2020, https://www.enigmasoftware.com/barium-group-threatens-millions-computers-stealthy-supply-chain-hacking-attacks/.

of PRC state-sponsored espionage so large that it is impossible to chart is identified[1096].

Stepping beyond the means of attack, the truly insightful point comes in how the PRC, through Barium, exploited this clandestine access. Whilst such access could have allowed the group to conduct devastating and lucrative ransomware attacks, reports indicate that under PRC direction it focused not only on spying but, in doing so, only spied on a fraction of the compromised systems. In the Asus case, for example, by identifying MAC addresses of interest Barium only accessed approximately 600 systems out of a total infected number of 600,000. Though open-source reporting does not confirm which organisations were targeted, the sheer breadth of the Barium attack, combined with its links to the PRC state, make it likely that those 600 were chosen due to their specific intelligence yield[1097].

Whilst one might assume that this form of attack could only be effective against unaware individuals or organisations with limited cyber security provision, the reality is that other similar state-sponsored attacks are known to have compromised Defence contractors, Governments, and militaries. Often through a failure to effectively employ routine cyber security practices such as patch management and sandboxing, compromises continue to offer the PRC huge value in cyber espionage[1098]. With further examples including the 2014 PRC breach of the US Government's OPM, there is little doubt that the 'Chinese way' of employing cyber capabilities in grey zone conflict is highly impactful[1099].

[1096] For depth on the Barium attacks, see:
A. Greenberg, "A Mysterious Hacker Group Is on a Supply Chain Hijacking Spree", *Wired* 3 May 2019.
L. Newman, "Inside the Unnerving Supply Chain Attack That Corrupted Ccleaner", ibid., 17 April 2018.
Y. Aung, "Operation Shadowhammer", ed. SecureList (Kaspersky 2019).

[1097] For the focus of the Barium attacks, see:
GoldSparrow Barium Group Threatens Millions of Computers through Stealthy Supply Chain Hacking Attacks.
R. Lakshmanan, "New Study Links Seemingly Disparate Malware Attacks to Chinese Hackers", *The Hacker News* 5 October 2021.

[1098] For depth on patch management, see:
UK, "Vulnerability Management ", ed. National Cyber Security Centre (2022).
For depth on sandboxing, see:
Hysolate, "Sandbox Software Development: Use Cases and Techniques ", (Hysolate, 2022).

[1099] For depth on the OPM attack which accessed US Federal systems and compromised approximately 22 million records on employees, contractors, and their families, see:
M.S. Schmidt, D.E. Sanger, and N. Perlroth, "Chinese Hackers Pursue Key Data on Us Workers", *The New York Times* 7 March 2014.
R.J. Harknett, Smeets, M. , "Cyber Campaigns and Strategic Outcomes", *Journal of Strategic Studies,* (2020): 21.

Known to have already advanced PRC air power to a point of near parity with the West, such developments are recognised as having shifted the strategic balance in the Asia-Pacific. Based on this, it can be assessed with confidence that the PRC is highly likely to continue its targeting of Western adversaries through these well proven cyber espionage capabilities.

Looking beyond cyber espionage, the PRC's ability to achieve disruptive cyber attacks against the West has also been increasingly proven. Though not directly impacting military capabilities such as air power, these means are focused on the type of left-of-launch vectors which dovetail into the PRC's approach to grey zone conflict. As shown in Part 2 of the thesis, these means could credibly disrupt air power.

An example is the alleged PRC-directed cyber attacks against Indian infrastructure in 2020. Reported widely in the media, it was assessed that following India-PRC clashes along their disputed border in October 2020 there was a significant increase in cyber attacks against not only Indian government, defence, and public sector organisations but also CNI[1100]. Delivered via trojan horse malware originating from PRC-sponsored hackers, attacks against the Indian Maharashtra State Electricity Board (MSEB) are for example alleged to have caused servers to crash leading to mass blackouts in Mumbai[1101]. Whilst subsequent analysis suggested that the actual cause of the blackouts may have been human error, the existence of malware originating from the PRC on MSEB

J. Brenner, interview by J. Chaffetz, 2016.
J. Devanny, Martin, C., Stevens, T., "On the Strategic Consequences of Digital Espionage", *Journal of Cyber Policy,* 6, no. 3 (2021).
US, "The Opm Data Breach: How the Government Jeopardised Our National Security for More That a Generation", ed. US House of Representatives Oversight and Government Reform Committee (2016).
For arguments that information alone gained through cyber espionage do not help the PRC rebalance strategic advantage, see:
R. Farley, "Theft Can't Help China's Air Force Build Quality Engines", *The National Interest,* (2021).

[1100] For *The New York Times* report, see:
Sanger, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out".
For background on the border clashes, see:
Staff-Writer, "India-China Dispute: The Border Row Explained".

[1101] "Mumbai Power Outage in October May Have Been Result of 'Cyber Sabotage'".

servers confirmed the growing PRC intent and capability to direct cyber attacks against state adversaries[1102].

Adding further evidence, CISA reported in 2021 how PRC sponsored hackers were behind 13 confirmed cyber compromises of networks belonging to US commercial oil and natural gas (ONG) pipeline operators. Using a combination of social engineering and technical means, CISA assessed that the activity was designed to confirm that the PRC could, via cyber means, hold US pipeline infrastructure at risk. In doing so, the activity proved how the PRC is actively preparing to expand the type of disruption achieved in India to Western adversaries with whom it may soon come into conflict with[1103]. In doing so, it would achieve a viable left-of-launch attack vector which, by targeting military CNI, could ground air platforms. Beyond this it could also, through wider employment against all capabilities, credibly shift the strategic Asia-Pacific balance of power.

Stepping beyond such clandestine activity, the PRC is now also openly signalling its ability to harness cyber capabilities through public hacker events including the Tianfu Cup[1104]. Indicating that the PRC has reached a position at which it is comfortable to showcase its capabilities, the shift can be interpreted as a new development in which the PRC is choosing to use cyber as a means of deterrence to dissuade Western military action in its near abroad. By building on previous evidence such as the India power and ONG attacks, events including the Tianfu Cup communicate to the West that the PRC is now a cyber power to be reckoned with.

Given the developments discussed above, Western adversaries are induced to question whether military operations launched in the Asia-Pacific would be

[1102] Reporting which suggests the blackouts were human errors include:
"'It Was Human Error': Cyberattacks Too Place but Didn't Cause Mumbai Outage Says Govt", *The Times of India*, 2 March 2021.

[1103] For detail on the ONG pipeline attacks, see:
US, "Alert (Aa21-201a): Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013", ed. Cybersecurity and Infrastructure Security Agency (CISA) (2021).

[1104] The Tianfu Cup is a PRC sanctioned annual hacking competition which is assessed to be designed to openly demonstrate the PRC's ability to hold key Western systems and networks at risk. For detail, see:
Tianfu Cup, "Tfc - International Cyber Security Forum", http://www.tianfucup.com/en/#canjia.
J.D. Work, "China Flaunts Its Offensive Cyber Power ", *War on the Rocks,* (2021).
D. Winder, "Iphone 13 Pro Hacked: Chinese Hackers Suddenly Break Ios 15.0.2 Security", *Forbes* (2021).
E. Kovacs, "$1.9 Million Paid out for Exploits at China's Tianfu Cup Hacking Contest", *Security Week,* (2021).

credibly disrupted to the point of non-viability by PRC cyber means. If such deterrence messaging were successful, the PRC's grey zone intent of shifting the strategic balance and preventing conflict before a shot is fired takes a decisive step forward. Through this the PRC may never have to prove the viability of its cyber capabilities with the cyber threat alone enough to prevent conflict and achieve its political aims.

Conclusion on the PRC's Cyber Threat to Western Air Power

Opening the discussion of cyber threats to Western and aligned air power, this section considered the PRC. Initially characterising Western-Sino relations as one in which the West is perceived to be a hegemonic force driven by a neo-interventionist intent, and the PRC an aggressive and expansionist power, a clash is predicted that will 'shape geopolitics for decades'[1105]. Exploring how the PRC cyber threat will influence this, it was concluded that though grey zone in nature the PRC maintains cyber capabilities able to have strategic impact. Notably, cyber means are predicted as forming a key element of deterring the West from militarily challenging the PRC's regional aspirations.

With this reality informed by a militarily rising PRC closing the gap on the historically dominant West, it becomes likely that relations may be unbalanced through cyber. Ranging from espionage through A2AD to counter-space, such cyber means have the potential to offer the PRC strategic advantage including the necessary disruption of Western air power. Through this the PRC's grey zone approach is identified as forming a blueprint for a rising power to use cyber means to achieve its goals without resorting to armed conflict.

[1105] Jones, "Global China: Assessing China's Growing Role in the World."

Russia

Introduction to the Russian Cyber Threat

Continuing from the above discussion of the PRC, this section will consider the Russian cyber threat to Western air power. Beginning with an examination of how Russian-Western relations have degraded due to NATO's eastward expansion, the discussion will set up an exploration of whether these tensions have created a credible cyber threat emanating from the Russian state.

Discussed in two parts, the Russian cyber threat will be explored before its cyber capabilities are considered. Finally summarising, the section will conclude that tensions, competition and conflict between Russia and the West are inevitable due to Russia's intent to regain influence. Further to this, it will also be highlighted that the means of pursuing this intent are underpinned by a nonlinear strategy. This strategy, it will be noted, is anchored by credible cyber capabilities and a likelihood that Russia will learn from its underwhelming cyber performance during the 2022 invasion of Ukraine. When combined with the final factor of Western air power being keystone to deterring Russia, it will ultimately be assessed that Russia presents a credible cyber threat to Western air power.

Russian-Western Relations

In the post-Cold War 1990s a new partnership between Russia and the West appeared to be forming with the primary question being not whether a relationship would be pursued, but what form this would take[1106]. Despite this promise, Russian-Western relations quickly soured in the 1990s as the ex-Soviet Republics looked westward for the freedoms and stability that a struggling Russia could not provide. Cemented by the collapse of the Warsaw Pact in 1991, these states quickly identified NATO as a 'bright pole of intense attraction' offering a

[1106] For depth on post-Cold War Russian-Western relations, see:
A.C. Lynch, "The Evolution of Russian Foreign Policy in the 1990s", *The Journal of Communist Studies and Transition Politics,* 18, no. 1 (2002).

'meaningful, democratic and effective structure' through which to engage in a new European security system[1107].

This Eastern European intent was quickly met by a Western desire to expand its influence. In contrast Russian leaders were appalled, claiming that the West was breaking assurances not to expand into its traditional sphere of influence[1108]. Despite many in the West also considering the decision a 'fateful error', expansion was actively pursued[1109]. By 2004 this led to NATO's inclusion of the Czech Republic, Hungary, Poland, Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia, and Slovenia[1110].

An affront to Russia, the scene was set for a deterioration of Russian-Western relations[1111]. Manifested in examples including Russia's 2008 conflict with Georgia, 2014 seizure of Crimea and 2022 invasion of the wider Ukraine, a reality emerged in which Russian-Western relations are strained to a point of diplomatic tension, economic sanctions, and a credible potential of armed conflict[1112]. Within this context, the key question for this discussion is whether, as part of these

[1107] For the first quote, see:
G.B. Solomon, *The Nato Enlargement Debate, 1990-1997* (Westport Praeger 1998), 7.
For the second quote, see:
L. Havel, "Speech to the Czech and Slovak Federal Assembly on Thursday 10 May 1990", ed. Czech and Slovak Federal Assembly (Council of Europe (Speeches) 1990).

[1108] For ex-Soviet official's comments, see for example Anatoli Admamishin, Soviet Deputy Foreign Minister who is quoted in:
M. Kramer, "The Myth of a No-Nato-Enlargement Pledge to Russia", *The Washington Quarterly* 32, no. 2 (2009): 40.
Russian claims that promises were broken were supported by ex-US officials, notably Robert McNarmara. For detail, see:
R.S. McNamara, Blight, J.G., *Wilson's Ghost: Reducing the Risk of Conlfict, Killing and Catastrophe in the 21st Century* (New York Public Affairs, 2001).

[1109] For the quote, see:
G.F Keenan, "A Fateful Error", *The New York Times*, 5 February 1997 1997.
For supporting depth, see:
Eisenhower-Group, "Open Letter: Opposition to Nato Expansion", *Arms Control Association,* (1997).

[1110] For NATO expansion, see:
NATO, "Member Countries".
For Western arguments against NATO expansion, see:
R.N. Haas, "Enlarging Nato: A Questionable Idea Whose Time Has Come ", *Brooking Institute* (1997).

[1111] It is noted that others offer a counterargument to NATO expansion being the cause of poor Russian-Western relations. For an example of this alternative views, see:
D. Trenin, "Russia's Line in the Sand on Syria: Why Moscow Wants to Halt the Arab Spring ", *Foreign Affairs* (2012).

[1112] For analysis of this period, and the increased likelihood of Russian-Western conflict, see:
K. Marten, "Nato Enlargement: Evaluating Its Consequences in Russia", *International Politics,* 57 (2020): 420.
S.M. Walt, "Nato Owes Putin a Big Thank You ", *Foreign Policy,* (2014).
For an example of how the West characterises the increasing Russian threat, see:
UK, "Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy", 16.
For an example of where this potential for Russian-NATO conflict is most advanced in the Ukraine, see:
P. Kirby, "Is Russia Preparing to Invade Ukraine? And Other Questions", *BBC News Online*, 12 January 2021.

tensions, Russia poses a credible cyber threat to the West and, more specifically, its air power?

The Nature of the Russian Cyber Threat

Exploring the nature of the Russian cyber threat, the UK Parliament's Intelligence and Security Committee identified Russia as a highly capable cyber actor which 'aggressively undertakes cyber pre-positioning' to achieve its political aims[1113]. Expanding on this, Lindy Cameron, Chief Executive of the UK's NCSC, underlined the assessment identifying Russian intelligence services, and the state-sponsored groups within their control, as forming the greatest cyber threat to Western interests[1114].

The Russian activity described by Cameron is delivered through a range of both independent and famously territorial agencies alongside state linked malicious cyber actors operating on their behest[1115]. Notwithstanding these divisions, all Russian malicious cyber activity is at its core cohered by the Russian state, or more precisely the Kremlin, to achieve geo-political objectives[1116]. Through this cohesiveness, the Russian cyber threat may be disparate in application but is driven by three central strategic goals: to gather information, to probe for digital weaknesses and, ultimately, to weaken targeted states[1117].

[1113] UK, "Intelligence and Security Committee of Parliament: Annual Report, 2019-2021", ed. House of Commons (2021), 2.

[1114] L. Cameron, "Lindy Cameron Speaking at the Rusi Annual Security Conference", *NSCSC Speeches* (2021).

[1115] The principle Russian intelligence agencies are: Sluzhba Vneshnei Razvedki (SVR) responsible for foreign intelligence; Federal'naya Sluzhba Bezopasnosti (FSB) responsible for internal security; Glavnoe Razvedyvatel'noe Upravlenie (GRU) which is the intelligence arm of the Russian Armed Forces.

R.W. Pringle, "The Heritage and Future of the Russian Intelligence Community", *International Journal of Intelligence and Counter Intelligence,* 11, no. 2 (2008).

[1116] A. Foxall, "Putin Sees and Hears It All: How Russia's Intellgience Agencies Manace the Uk", *Henry Jackson Society,* (2018): 9.

[1117] For Russian political aims, see:

Russian Federation, "Strategy for the National Security of the Russian Federation up to 2020", ed. Government of the Russian Federation (2009).

For depth, see:

R. and Miron Thornton, M., "Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constrains Faced by the United Kingdom", *Journal of Cyber Policy,* 4, no. 2 (2019): 259.

MI5, "Intelligence and Security Committee of Parliament: Annual Report, 2016-2017", ed. HouseofCommons (2017), 55.

In considering how Russia translates this into action, an informative starting point is the writings of Gerasimov, Chief of the Russian General Staff[1118]. Though coined the 'Gerasimov Doctrine' by Galeotti, Gerasimov did not, as his critics argue and Galeotti himself acknowledges, deliver a new doctrine[1119]. Rather, in offering a cohesive extension of thinking established by his predecessor, Makarov, Gerasimov characterises Russia's doctrinal approach to state-on-state competition as non-linear in nature[1120].

Offering an informative lens through which to understand the Russian intent towards a 'vision of total warfare', Gerasimov combines political, diplomatic, economic, and other nonmilitary measures into a single spectrum[1121]. Encased in this, cyber means emerge as a key element able to discreetly reach across time, space, and activities to achieve strategic aims[1122]. When directed at Western interests, Heickero explains that this cyber threat could target 'centres of gravity and critical vulnerabilities' whose disruption could degrade military capability and political will without risking conventional escalation[1123]. In this manner, the cyber threat becomes an anchoring capability of the Russian arsenal which, as a collective force, is focused on the geopolitical aim of regaining regional influence lost to the West in the post-Cold War period[1124].

Whilst such assertions on the prominence of cyber were previously widely held, the invasion of Ukraine in February 2022 raised further questions. In advance of

[1118] For Gerasimov's writings, see:
V. Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations'", *Military-Industrial Kurier,* (2013).

[1119] For representative criticisms of the 'Gerasimov Doctrine', see:
M. Galeotti, "The Gerasimov Doctrine", *Berlin Policy Journal,* (2020).
Ng, N. and Rumer, E. 'The West Fear's Russia's Hybrid Warfare. They're Missing the Bigger Picture', *Carnegie,* 3 July (2019). Available at: The West Fears Russia's Hybrid Warfare. They're Missing the Bigger Picture. - Carnegie Endowment for International Peace (Accessed: 28 December 2021).

[1120] For a summary of Galeotti's coining of, and his subsequent difficulties with, the 'Gerasimov Doctrine', see:
M. Galeotti, 6 July 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.
For the lineage of thinking from Makarov to Gerasimov, see:
A. Monaghan, "The 'War' in Russia's 'Hybrid Warfare'", *Parameters* 45, no. 4 (2015): 68.

[1121] M.K. McKew, "The Gerasimov Doctrine", *Politico,* (2017).

[1122] Ibid.

[1123] R. Heickero, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations", *Swedish Defence Research Agency,* (2010): 52.

[1124] For cyber anchoring Russian activity, see:
S. G. and Bogdanov Chekinov, S. A. , "Прогнозирование Характера И Содержания Войн Будущего: Проблемы И Суждени", *Voennaya Mysl,* (2019).
K. and Seaboyer Giles, A. , "The Russian Information Warfare Construct", *Defence Research and Development Centre Canada,* (2019).

the conflict, commentators had, in reflecting on previous Russian displays of intent and capability through events such as the cyber targeting of the Ukrainian power grid in 2014, assessed that the conflict would mark the first true cyber war[1125]. In this, it was predicted, 'the Kremlin's cyber weapons' would be harnessed to 'cripple the Ukrainian government and deliver a decisive advantage on the battlefield'[1126]. However, in a similar vein to Russia's conventional under performance, the reality was less decisive.

Explored by Lewis, it is argued that the metric against which cyber attacks should be judged is not whether they achieved 'network penetration or the disruption of services or data' but if they materially aid conventional military attack. Going further, Lewis clarifies this by asserting that cyber impact in war can most accurately be gauged as a combination with Electronic Warfare (EW) in which it intends to 'degrade information advantage and intangible assets [such as data], communications, intelligence assets, and weapons systems to produce operational advantage'. By this metric, he concludes, Russia's employment of cyber in Ukraine provided little benefit[1127]. Cyber may therefore not be the Russian anchoring capability it has been argued to be.

In this context, Russia's cyber attack on the Viasat network in the opening hours of the conflict is illustrative. Deploying destructive AcidRain wiper malware against Viasat modems and routers, the attack attributed by US intelligence to the Russian GRU erased Master Boot Records (MRB) before rebooting and permanently disabling the machines[1128]. Characterised by the UK's Foreign Secretary, Liz Truss, as 'shocking evidence of a deliberate and malicious [cyber] attack', it impacted several thousand commercial customers in Ukraine and tens

[1125] For depth on the cyber attacks on the Ukrainian power grid in 2014, see:
A. and Lipovsky Cherepanov, R. , "Blackenergy – What We Really Know About the Notorious Attacks", *Virus Bulletin Conference,* (2016).

[1126] For a discussion of the failure of Russia to deliver true cyber war, see:
J. Wolff, "How Do We Know When Cyber Defenses Work? ", *Brooking Institute,* (2022).
For examples of pre-conflict analysis which suggested the likelihood of a Russian led cyber war, see:
M Miller, "Russian Invasion of Ukraine Could Redefine Cyber Warfare", *Politico* 28 January 2022 2022.

[1127] Lewis, "Cyber War and Ukraine".

[1128] For a discussion of the technical exploit in the Visat cyber attack, see:
P. O'Neill, "Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion", *MIT Technilogy Review,* (2022).
For an overview of the AcidRain malware, see:
Splunk, "Threat Update: Acidrain Wiper", (Splunk, 2022).

of thousands of fixed broadband customers in other European countries[1129]. When viewed in terms of Lewis' definition, this impact was arguably more significant. With the Ukrainian military widely reliant on Viasat at the time for command and control, its forces lost situational awareness and commanders were forced to physically move to their troops' positions to issue orders[1130].

Despite this, Ukraine acted immediately, stabilising the network in hours and achieving full stabilisation in days. With further proactive measures taken by Viasat to ensure other supporting applications were not impacted, the Viasat example is for many commentators assessed as indicative of a wider trend of Russian cyber attacks falling short of meeting Lewis's definition[1131].

Though further examples including DoS attacks on Ukrainian websites which were ultimately recovered within hours can be cited, the persistent deployment of malware by a group believed to be linked to the infamous Russian Sandworm APT continues the theme of consistent intent but limited impact[1132]. Initially reported by the Microsoft Threat Intelligence Centre (MSTIC) in January 2022 as an unidentified APT under the DEV-0586 designator, the group was using malware designed to look like ransomware. However, it lacked a ransom recovery mechanism to target Ukrainian organisations[1133]. Tracked over the following months by MSTIC, the APT now identified as IRIDUM re-emerged in October 2022. In this circumstance, IRIDUM was assessed to be using Prestige malware

[1129] Viasat Ka-Sat Network Cyber Attack Overview.

[1130] For Liz Truss's statement, see:
UK, "Russia Behind Cyber-Attack with Europe-Wide Impact an Hour before Ukraine Invasion".
For an assessment of the military impact of the Viasat attack, see:
P. Soone, "Battle for Kyiv: Ukrainian Valor, Russian Blunders Combined to Save the Capital", *The Washington Postg*, 24 August 2022.
For comment on US intelligence assessments of the Viasat attack, see:
G. Corera, "Russia Hacked Ukrainian Satellite Communications, Officials Believe", *BBC News* 25 March 2022.

[1131] R. Dalsjö, Jonsson, M., Norberg, J., "A Brutal Examination: Russian Military Capability in Light of the Ukraine War", (International Insstitute for Strategic Studies 2922).

[1132] For a discussion on DDoS attacks, see:
J. Tidy, "Ukraine Cyber-Attack: Russia to Blame for Hack, Says Kyiv", *BBC News* 14 January 2022 2022.

[1133] MSTIC uses the 'DEV' designations as a temporary name for an 'unknown, emerging, or developing cluster of threat activity'. Once MSTIC reaches a high confidence on the origin or identity of the actor behind the activity DEV is replaced by a named actor. Other organisations use similar processes but with differing naming conventions.
Microsoft, 8 November 2021, 2021, https://www.microsoft.com/en-us/security/blog/2021/11/08/threat-actor-dev-0322-exploiting-zoho-manageengine-adselfservice-plus/.

to target logistics organisations in Ukraine and Poland known to be moving humanitarian or military supplies into Ukraine[1134].

Though IRIDUM under its associated name of Sandworm had been formally linked to the GRU by US Court papers and high-profile attacks such as those on the Winter Olympics in 2018, no significant military impact against Ukraine was achieved by the group[1135]. Therefore, rather than reaching Greenberg's 2020 warning that Sandworm was the clearest example yet of a 'rogue actor advancing [towards] a cyberwar dystopia', its evolution as IRIDUM failed to have significant impact on the conflict in Ukraine[1136].

Given these examples, one must ask whether the Russian cyber threat is impotent? Responding to this, two counter-arguments can be made. Firstly, the lack of cyber impact may not reflect an impotent Russian cyber threat but a fundamental lack of coordination between cyber and conventional forces. With such coordination extolled as a necessity by UK doctrine, it is recognised that for cyber attacks to offer benefit they must be combined with other domains[1137]. However, when used in an ad hoc or uncoordinated manner as Russia appears to have done, cyber attacks prove less useful[1138].

In this context, the failure to achieve cyber impact in Ukraine could be assessed not as a lack of Russia cyber capability or intent. Rather, it may indicate a higher-level failure in the planning and staff work necessary to deliver effective coordination. An assertion supported by wider comments on Russian planning and delivery failures across all domains of operation in Ukraine, it becomes

[1134] "New "Prestige" Ransomware Impacts Organizations in Ukraine and Poland", (Microsoft, 2022).
[1135] For US Court Papers linking Sandworm to the GRU, see:
US, "Us District Court Western District of Pennsylvania - Us Vs Yuriy Andrienko ", (2020).
For depth on the Winter Olympics attack in 2018, see:
A. Greenberg, "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History", *Wired* 17 October 2018.
For depth on Sandworm and its development, see:
K Zetter, "Russian 'Sandworm' Hack Has Been Spying on Foreign Governments for Years", ibid., 14 October 2014 2014.
R. Holt, "Sandworm: A Tale of Disruption Told Anew", *We Live Security*, 21 March 2022.
[1136] A. Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Anchor Books 2020), xii.
[1137] For UK doctrine comments on the necessity to coordinate cyber with other conventional capabilities, see:
UK, "Joint Doctrine Note 1/18 - Cyber and Electromagnetic Activities", ed. Ministry of Defence (2018), 3.
For broader UK doctrine comment on the necessity to coordinate across domains, see:
"Joint Concept Note 1/20 - Multi-Domain Integration", ed. Ministry of Defence (2020).
[1138] Lewis, "Cyber War and Ukraine".

unsurprising that Russia did not effectively coordinate the complex space of offensive cyber operations. Further, if Russia effectively learns lessons from Ukraine and improves this underpinning operational facilitator, the cyber threat may emerge in future conflicts as the anchoring capability it has been predicted to be[1139].

Beyond this, Russia's underwhelming cyber impact may not be due to a lack of intent or capability but an impressive cyber defence. Forewarned by its experiences from 2014 onwards, Ukraine in partnership with Western states and technology companies proactively developed its cyber defences ahead of the 2022 conflict[1140]. Formalised by its 2016 Cyber Security Strategy, delivery of this coordinated activity has included examples such as US CYBERCOM's deployment of a 'hunt forward' capability.

Reacting to Western intelligence officials' identification of Russian military preparations and their concern that a conflict would be accompanied by 'a new blizzard of cyber attacks', forty US military personnel were deployed to Ukraine in 2021 to conduct 'hunt forward' activities on Ukrainian networks[1141]. Intending to achieve 'a front-row seat' for Russian cyber preparations, the personnel were pre-positioned prior to attacks materialising. In doing so, the US has been credited with ably assisting in the defence of the cyber domain, even whilst being precluded from operating in the conventional domains[1142].

This involvement in Ukrainian cyber defence has also extended to not just other Western nations but extensive commercial support. Drawing in a breadth of

[1139] For further discussion on Russia's failure to conduct effective military planning, coordination, and delivery in Ukraine, see:

S. Jones, "Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare", (Center for Strategic and International Studies 2022).
Dalsjö, "A Brutal Examination: Russian Military Capability in Light of the Ukraine War".

[1140] Lewis, "Cyber War and Ukraine".

[1141] For the quote, see:

G. Corera, "Inside a Us Military Cyber Team's Defence of Ukraine", *BBC News* 30 October 2022.

For a wider overview of US CYBERCOM 'hunt forward' activity including its objectives and impact in Ukraine, see:

US, "U.S. Conducts First Hunt Forward Operation in Lithuania", ed. US Cyber Command (2022).
B.D. Williams, "Cybercom Has Conducted 'Hunt-Forward' Ops in 14 Countries, Deputy Says", *Breaking Defense*, 10 November 2021.
P.M. Nakasone, interview by L. Johnson, 5 April 2022.

[1142] Corera, "Inside a Us Military Cyber Team's Defence of Ukraine".

companies including Microsoft, BitDefender, Google and Sophos, activities from remote network defence, through threat intelligence to capacity building have enhanced the defensive posture[1143]. When built atop of an already impressive Ukrainian national cyber capability forged through years of Russian cyber aggression, the relative lack of Russian cyber success can be assessed as not a failure in intent or capability, but a triumph in cyber defence.

Considered in this context, it can be assessed that the lesson from Ukraine is not that the Russian cyber threat is non-existent, but that an effective cyber defence is capable of blunting even the most credible of attacks. To understand the depth and ability of the potential Russian threat, and whether once lessons are learnt it may still pose a credible cyber threat to Western air power, Russia's cyber capabilities must next be examined.

Russia's Cyber Capabilities

Despite harbouring a strategic intent to regain influence through the application of cyber means, to achieve its aims and dismiss the criticisms of its performance in Ukraine Russia must also hold the necessary cyber capabilities. Charting the development of these, the first known credible Russia cyber threat to the West was the 1998 Moonlight Maze attack. Widely considered the first large-scale act of cyber espionage by a state actor, Russia conducted a sustained probing of US Pentagon systems over a two-year period. Reported to have compromised 5.5 gigabytes, or 3 million pages, of unclassified yet sensitive military documents, it offered an early demonstration of Russia's credible cyber capability[1144].

[1143] For Ukraine's Cyber Security Strategy, see:
Ukraine, "Cyber Security Strategy of Ukraine", ed. President of Ukraine (2016).
For background on Microsoft's assistance to Ukraine and examples of threats identified, see:
Digital Security Unit, "Special Report: Ukraine - an Overview of Russia's Cyberattack Activity in Ukraine ", (Microsoft 2022).
Microsoft Threat Intelligence Center, "Destructive Malware Targeting Ukrainian Organizations", (Microsoft, 2022).

[1144] For depth on Moonlight Maze, see:
O. Haizler, "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking", *Cyber, Intelligence and Security,* 1, no. 1 (2017): 34.
F. Kaplan, *Dark Territory: The Secret History of Cyberwar* (New York Simon and Schuster, 2016), 85.

Though Moonlight Maze did not cause direct damage to military capabilities, it could in theory have offered Russia a decisive edge in conflict. In relation to air power, for example, information gained may have offered details on how to degrade, disrupt, and destroy air capabilities. Given the potential impact this advantage could achieve, it is notable that Russia has continued to develop and operationalise the capability.

A more recent example of such development is Agent.BTZ. First reported in 2008, Agent.BTZ is a form of malware known to originate from the Russian state. Believed to have been introduced to secure air gapped US military systems by a US employee in Afghanistan using an infected USB thumb drive, it spread undetected to classified and unclassified US and wider NATO networks[1145]. Forming a 'digital beachhead' from which Russia could exfiltrate live data, Agent.BTZ could if exploited during a crisis have undermined Western military capabilities, including air power[1146].

In response to this growing cyber capability, Western states have since 2018 been increasingly vocal in confirming attacks on their systems and networks. Through this 'naming and shaming' strategy, one of the most prevalent and capable identified Russian cyber units is the GRU's 85th Main Centre for Special Technologies. Commonly referred to by its Russian language initials of GTsST, it has publicly been identified as a state-back hacking crew operating under numerous pseudonyms. With these including the aforementioned Sandworm alongside a breadth of others including BlackEnergy, Telebots, VoodooBear and FancyBear, the damage caused has been characterised as 'reckless, indiscriminate…and without regard for international law'[1147].

[1145] F-Secure, "Worm:W32/Agent.Btz'", in *Threat Descriptions* (2022).

[1146] For quote, see:
W. Lynn, "Defencing a New Domain", *Foreign Affairs,* (2010).
For depth on Agent.BTZ, see:
E. Nakashima, "Defense Official Discloses Cyberattack", *Washington Post*, 24 August 2010.
"Cyber-Intruder Sparks Massive Federal Response and Debate over Dealing with Threats", *Washington Post*, 9 December 2011.

[1147] For quote, see:
D. Raab, "Uk Condemns Russia's Gru over Georgia Cyber-Attacks'", ed. Gov.UK - Press Release (2020).
For warnings on the threat from the GRU and cover names used, see:
J. Hunt, "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed", ed. Gov.UK Press Release (2018).

Examining some of the events that have with 'the highest level of probability' been attributed to GTsST, the most serious include its persistent undermining of Ukrainian sovereignty. Of note, this includes attacks on the national power grid in 2015 and 2016 alongside attacks on the financial, energy, public sector and key transport hubs in 2017[1148]. With similar reporting on the destructive and malicious nature of GTsST activity continuing to be published, a step change has been observed. Specifically, Russian cyber capabilities have shifted in nature and ability from the espionage focus of Moonlight Maze and Agent.BTZ to a more direct and operational form[1149].

Despite the apparent clarity of these developments, some commentators argue that Russia has not yet shown an ability to cause credible damage to military capabilities through cyber means. Charting known Russian cyber activities to evidence this, Fabian notes that the well-reported Russian cyber attacks in Estonia in 2007 and Georgia in 2008 did little more than harass the target states[1150]. Based on this, and supported by the above discussion on its cyber performance in Ukraine in 2022, it could be concluded that whilst Russian cyber activity is significant and may be advancing at pace, it remains in the military space a low-level and opportunistic activity[1151].

[1148] For depth on attacks against the power grid in 2015 and 2016, commonly referred to as BlackEnergy, see:
Cherepanov, "Blackenergy – What We Really Know About the Notorious Attacks".
For depth on attacks on financial, energy and public sectors in 2017, commonly referred to as the NotPeya attacks, see:
E. Nakashima, "Russia Military Was Behind 'Notpeya' Cyberattack in Ukraine, Cia Concludes", *Washington Post*, 12 January 2018.
I. Thomson, "Everything You Need to Know About the Petya, Er, Notpetya Nasty Trashing Pcs Worldwide", *The Register,* (2017).
For depth on attacks on transport hubs in 2017, commonly referred to as the Bad Rabbit attacks, see:
C. Brook, "Bad Rabbit Ransomware Hits Russia, Ukraine", *Digital Guardian,* (2020).
Kaspersky, "Bad Rabbit Ransomware", *Kaperskylabs: Secure List,* (2017).

[1149] Reporting produced by NATO members on GTsST includes a joint US-UK intelligence Cybersecurity Advisory note published in 2021 that identified GTsST as being behind the exploitation of the Kubernetes cluster attack. This led to 'widespread, distributed, and anonymised brute force access attempts against hundreds of government and private sector targets worldwide'.
NSA, "Russian Gru Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments".

[1150] For this argument, see:
S. Fabian, "The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy", *Defense and Security Analysis,* 35, no. 3 (2019).
For depth on cyber attacks against Estonia in 2007, see:
J.A. Lewis, "Cyber-Attacks Explained", *Centre for Strategic and International Studies,* (2007).
For depth on cyber attacks against Georgia in 2008, see:
R.J. Delbert, Rohozinski, R. and Crete-Nishihata, M. , "Cyclones in Cyberspace: Information Shapin and Denial in the 2008 Russia-Georgia War", *Security Dialogue,* 43, no. 1 (2012).

[1151] Fabian, "The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy", 322.

In contrast to this conclusion, NATO has argued that whilst the targeting of Western capabilities through cyber is 'strikingly absent' from Russian national strategies, Russia remains likely to hold the capabilities to do so[1152]. Therefore, rather than Russia not being able to target Western military capabilities through cyber the reality is, in NATO's assessment, that Russia has chosen not to do so. This decision is not, their analysis concludes, due to some form of moral or legal restraint, but because Russia recognises that by using offensive cyber against Western militaries it is likely to 'trigger red lines' and raise the stakes of cyber conflict[1153].

In considering this, an examination of strategic statements made by some Western states suggests that despite Russia's reticence to 'cross the cyber line', the West itself is increasingly likely to cause such escalation. Talking in 2010 Nick Harvey MP, the UK's Minister of State for the Armed Forces, confirmed that the UK's cyber intent included exploiting its adversaries by replacing 'the precise and tailored effects of a conventional attack' with cyber attacks[1154]. Leading to a later acknowledgement of a formal offensive cyber programme, the UK, like many of its Western allies, has openly expressed its intent to 'cross the cyber line'[1155].

Going further, evidence from 2018 indicates that through a US CYBERCOM operation which targeted the St Petersburg based Internet Research Agency (IRA), the West may already have begun this escalation. Overtly private but widely acknowledged as run by Russian-intelligence, the IRA is credited with being behind the manipulation of social media in the run up to the 2016 US Presidential election. Acting in response, the US is widely confirmed to have used offensive cyber means to significantly damage IRA systems causing a loss of data and operational failures[1156]. Described as an 'unprecedented milestone in

[1152] For the quote, see:
K. Giles, "'Information Troops: A Russian Cyber Command?", *3rd International Conference on Cyber Conflict,* (2011): 49; J. Hakala, Melnychuk, J., "Russia's Strategy in Cyberspace", *NATO Cooperative Cyber Defence Centre of Excellence,* (2021).

[1153] "Russia's Strategy in Cyberspace", 5.

[1154] N. Harvey, interview by K. Giles, 2011.

[1155] For an overview of the UK's National Offensive Cyber Programme, see:
UK, "National Cyber Force Explainer ", ed. National Cyber Force (2021).
For comments on crossing the 'cyber line', see:
P. Sanders, interview by D. Sabbagh, 25 September 2020.

[1156] For confirmation of the action against the IRA, see:

the history of cyber conflict', the action may not have impacted Russian military capabilities[1157]. However, what it did cause was a 'militarisation of the internet' which, in Olejnik's assessment, will significantly increase the likelihood of escalation from both Russia and the West[1158].

With other examples of the West threatening Russia with offensive cyber means including the UK's reaction to the 2018 alleged GRU poisoning of Skripal in Salisbury, a clear picture emerges[1159]. Specifically, Russia has shown through Moonlight Maze to Agent.BTX the capability to compromise and impact Western military networks and systems. It has also shown through events from Georgia to Ukraine that it is willing to employ such means to achieve its 'vision of total warfare'[1160].

Though its underwhelming 2022 cyber performance in Ukraine has led to questions over its ability to deliver such aims, and open-source reporting is yet to show a further militarisation of Russian cyber capabilities, a clear combination of cyber intent and capability has been demonstrated. Therefore, when taken collectively with the West pushing the cyber line, it can be assessed that Russia has not only the ability to step beyond previous 'red lines' on the militarisation of cyber, but also the motivation to do so in reaction to a perceived Western provocation. Especially if enhanced by lessons learnt in Ukraine, the cyber targeting by Russia of Western military capabilities, including air power, becomes a credible possibility.

Russian Federation, "Us Cyber Attack on Fan: Details of the Failed Operation Us Cyber Command", ed. Federal News Agency (2019).
P.M. Nakasone, "Statement of General Paul M. Nakasone, Commander United States Cyber Command, before the Senate Committee on Armed Services", ed. Senate Committee on Armed Services (2019).

[1157] L. Olejnik, "Global Consequences of Escalating Us – Russia Cyber Conflict", *Council on Foreign Relations,* (2019).

[1158] For Olejnik's assessment, see:
L. Olejnik, "Target Confirming an Offensive Cyber Operation", *Security Privacy and Tech Inquirie,* (2019).
Olejnik, "Global Consequences of Escalating Us – Russia Cyber Conflict".

[1159] For the UK's response to the poisoning and its threats to use offensive cyber means against Russia, see:
T. May, "Pm Commons Statement on Salisbury Incident", ed. Gov.UK (2018).
B. Johnson, interview by J. Lawless, 13 March 2018.
J. Lawless, "Sanctions, Cyberattack among Possible Uk Moves on Russia", *AP News*, 13 March 2018.
N. Carter, interview by E. MacAskill, 22 January 2018.

[1160] McKew, "The Gerasimov Doctrine".

Conclusions on the Russian Threat to Western Air Power

Continuing the discussion of cyber threats to Western air power, this section considered Russia. Having outlined increasing Russian-Western tensions, the role of the Russian cyber threat to Western air power was explored. Though balanced by a counterargument of Russia’s underwhelming cyber performance in Ukraine, the cyber threat was identified as an anchoring capability for a state focused on regaining regional influence. Tested through an exploration of Russia’s development of its cyber capabilities and how these could undermine Western air power, it was concluded that Russia has reached a point at which it poses a credible cyber threat which enhances the risk to Western air power.

Through the above narrative it is evident that tensions, competition and conflict between Russia and the West will continue to grow. It is also evident that for Russia its intent is underpinned by a nonlinear strategy anchored by cyber capabilities, and for the West its military lever is grounded in the keystone capability of air power. Taken collectively, it is therefore assessed that Russia is likely to learn from its underwhelming cyber performance in Ukraine and, in the event of tensions overflowing to direct conflict, cyber will emerge as a significant factor in Western air power’s cyber risk.

Iran

Introduction to the Iranian Cyber Threat

Concluding the examination of cyber threats to Western air power, this section discusses Iran. Initially summarising Western-Iranian relations which since 1979 have been dominated by anti-Western sentiments, the discussion next examines the nature of the Iranian cyber threat. Learning from events including the Stuxnet attack, it will be noted that a 1,200 percent increase in Iran’s spending on cyber aligned to an asymmetric approach makes Iran a ‘high [cyber] intent but low capability’ actor who could attempt to target Western interests[1161]. Showing an

[1161] Voo et al., "National Cyber Power Index 2020", 11.

ability to do so despite its low capability in the 2011 cyber attack on a US Sentinel UAV, it will be concluded that this intent may extend to Western air power.

Taken collectively, the section will conclude that Iran does not pose as credible a cyber threat as either the PRC or Russia. However, it could through a combination of cyber and conventional capabilities harass and disrupt Western air power. If conducted at a strategically vital moment, it will be asserted that such activity may allow a tactical victory, embolden Iran, and reinforce its hard-line leadership. By doing so, a shift in Middle Eastern strategic calculations may occur.

Iran-Western Relations

Until the end of the 1970s Western relations with Iran had been strong with US President Carter describing the country in 1977 as 'an island of stability in one of the most troubled areas of the world'[1162]. However, the Iranian Revolution of 1979 saw Shah Mohammed Reza Pahlavi replaced by Grand Ayatollah Ruhollah Khomeini. A Shiite cleric opposed to all Westernisation, his rise shifted the nation from a pro-Western monarchy to an anti-Western Islamic theocracy[1163].

Creating an acrimonious Western-Iranian relationship with only a few highpoints throughout the 1980s and 90s, these tensions would ultimately be cemented in 2002 with US President GW Bush's State of the Union address[1164]. Delivered on 29 January 2002, Bush would in this speech brand the 3 countries of North Korea, Iran, and Iraq as 'rogue states' who between them had created an 'axis of evil' responsible for harbouring, financing, and aiding terrorism[1165]. Politically motivated in the context of a post-9/11 US looking for an identifiable enemy to pursue, subsequent analysis shows the 'Axis of Evil' assertion to be flawed.

[1162] J. Carter, interview by A. Glass, 30 December 2018, 1977.

[1163] Staff Writer, "Us Relations with Iran ", *Council on Foreign Relations,* (2021).

[1164] Limited high-points and a 'mini détente' in the 1990s included Iranian President Mohammad Khatami's 1998 address to the UN General Assembly to call for a dialogue on terrorism and the US Secretary of State Madeleine Albright's high-level diplomatic meetings with Iran also in 1998. For President Khatami's address to the UN, see:

> M. Khatami, "Statement by H.E. Mohammad Khatami President of the Islamic Republic of Iran before the 53rd Session of the United Nations General Assembly New York, September 21, 1998", (Pars Times 1998).

For Secretary of State Albright's diplomatic meeting with Iran, see:

> L. Myers, "Albright, Ian Minister Meet", *AP*, 22 September 1998.

[1165] A. Glass, "President Bush Cites 'Axis of Evil,' Jan. 29, 2002", *Politico* (2019).

Driven not by logic but a political need to act, Bush's 'graphic, biblical terms' may have been unjustified but still confirmed enduring Western-Iranian tensions[1166].

Though both Iran and the West have since 2000 stoked these tensions, what is clear is that this was a pivotal moment through which the potential for conflict increased[1167]. When taken alongside regional battles for influence between Iran and the Western ally of Saudi Arabia, and proxy wars in Yemen and Syria, the likelihood of Western-Iranian hostilities comes even closer[1168]. An assessment underlined by the Iranian constitution which sets its national intent as 'an ideological mission of jihad…[to extend] God's law throughout the world'[1169], and Western politicians characterising Iran not as 'a state with an ideology, but…an ideology with a state'[1170], a viable question emerges of not when, but how, a Western-Iranian conflict may play out. When placed in the context of this thesis, one is led to ask what role cyber may play in such a conflict and whether through such means Iran could hold Western air power at risk.

The Nature of the Iranian Cyber Threat

Though these tensions between Iran and the West, especially between Iran and the US, have for many years created the potential of conflict, Kennedy assesses that whilst both want to appear strong and exert influence in the Middle East, neither want war. For the US, this is built on a desire to avoid destabilising the region and being forced to manage the aftermath, as it had to in Iraq. Alternatively, for Iran, this is built on the fact that it knows it cannot withstand a war against the West[1171]. Therefore, whilst Iran's nuclear developments may often take the headlines, the persistent conflict between

[1166] B. Woodward, *Plan of Attack* (New York: Simon and Schuster 2004), 84.
D. Frum, "The Enduring Lessons of the 'Axis of Evil' Speech", *The Atlantic,* (2022).

[1167] Examples of the West stoking tensions include US President Trump's removal of the US from the Joint Comprehensive Plan of Act (JCPOA) in 2018 calling it 'decaying and rotten' alongside the US's designation of Iran's Islamic Revolutionary Guard Corps (IRGC) as a terrorist group in 2019. Alternatively, from Iran, this has included attacks on Western shipping in the Strait of Hormuz and the shooting down of a US surveillance drone both in 2019.
For detail on the JCPOA, see:
K. Davenport, "The Joint Comprehensive Plan of Action (Jcpoa) at a Glance", (Arms Control Association 2022).
For Trump's view on the JCPOA, see:
D. Trump, interview by Staff Writer, 2018.

[1168] Staff Writer, "What Comes Next in the Standoff between the U.S. And Iran?", *World Politics REview,* (2022).

[1169] Islamic Republic of Iran, "Constitution of the Islamic Republic of Islam ", ed. Islamic Parliament of Iran (1979).

[1170] T. Blair, "Don't Make the Mistake of Dismissing Iran's Ideology ", *Washington Posr* 8 February 2019.

[1171] D. Kennedy, "How Iran Would Wage Cyber War against the United States", *The National Interest,* (2019).

these ideologically opposed sides is most likely to be fought in an asymmetric space in which impact can be achieved, but escalation avoided. Within this, cyber is increasingly becoming a focus for Iran[1172].

This focus on cyber centric asymmetric competition can also be explained by reflecting on Iran's geopolitical situation. Specifically, despite its geographically strategic position and shared interests with the PRC and Russia, neither of these great powers are likely to directly assist Iran in its struggle with the West[1173]. Further, even though Iranian President Raisi has stressed an intent to foster closer relations with his neighbours, Iran also has no state-level regional allies likely to support it[1174]. Given this, Iran in any direct conflict with the West is likely to be isolated. Therefore, finding asymmetric means such as cyber to achieve its strategic intent becomes key.

Beyond these strategic considerations, a further driver behind Iran's development of cyber capabilities was the 2010 Stuxnet malware attack on its Natanz uranium-enrichment plant[1175]. Believed to have been conducted by Israel and the US to disrupt the Iranian nuclear programme, Stuxnet laid bare the potential cyber impact the West and its allies could have on Iran. Leading Iran to identify cyber as a major pillar of its military strategy, the move not only recognised the importance of cyber but led to a rapid improvement of Iranian cyber capabilities[1176].

Though these factors establish the growing importance of cyber to Iran, its applicability to countering conventional Western military force, particularly air power, is not immediately clear. With Iran significantly outmatched by its Western adversaries, and with it seeking to use cyber in a sub-threshold manner to have

[1172] Ibid.

[1173] For depth on Iranian-Sino relations, see:

S. Hamrah, Eliasen, A. , "The China-Iran Strategic Partnership: 40 Years in the Making", *The Diplomat,* (2021).

For depth on Iranian-Russian relations, see:

A. Vatanka, "A New Chapter for Iran and Russia", *Foreign Policy,* (2022).

[1174] Iran's main regional ally is Hezbollah, but this group lacks state level resources. For an analysis of Iran's regional relations and allies, see:

S. Jafari, "Iran's Middle East Influence May Actually Be Declining", *Atlantic Council* (2021).

[1175] H. Ajilli, Rouhi, M. , "Iran's Military Strategy ", *Survival* 61, no. 6 (2019): 141.

[1176] Ibid.

impact without escalation, one might conclude that there is limited relevance. However, such an assumption would be incorrect.

Firstly, holding a genuine belief that the West poses an existential threat to its theocracy, Iran, despite recognising the damage war would do, continues to consider a conventional attack likely. Furthermore, when it comes, Iran believes that it will be US led[1177]. In such circumstances, the Iranian assessment is that US strategy would emphasise the suppression of enemy air defences and the conduct of air operations in the early phases of a conflict[1178]. To counter this, analysts suggest that Iran has designed an asymmetric strategy conceptually underpinned by A2AD[1179]. Whilst this includes conventional means to prevent or deter its adversaries access to airspace, its establishment of cyber as one of 5 operational A2AD pillars confirms a recognition of the domain's importance in countering Western air power[1180].

Secondly, looking beyond A2AD, the nature of the Iranian cyber threat to Western air power extends into periods of heightened tension, but not necessarily conventional warfare. Continually contesting its influence in areas including the Strait of Hormuz, and seeking to secure its own airspace from intrusion, Iran has shown intent and capability to use cyber to target Western air power[1181]. With the downing of a US Sentinel UAV in December 2011 illustrating this, the nature of the Iranian cyber threat, and its potential to impact Western air power, becomes evident.

Reflecting on this conceptualisation of Iran, and noting that since Iranian President Hassan Rouhani took office in 2013 spending on cyber has increased by 1,200 percent, there is little ambiguity that Iran's intent is to be a rising cyber power [1182] . With this underpinned by an annual Iranian cyber budget of

[1177] Ibid.
[1178] Ibid.
[1179] Ibid.
[1180] Iran's 5 A2AD pillars are: fixed and mobile air defence, artillery and ballistic missiles, electronic and cyber warfare, limited use of airpower, and naval combat.
Ibid.
[1181] Kennedy, "How Iran Would Wage Cyber War against the United States".
[1182] For the downing of the US UAV, see:
Ajilli, "Iran's Military Strategy ", 141.

approximately $19.8 million, and a promise for the Islamic Revolutionary Guard Corps (IRGC) to train 1,500 'cyber warriors', some commentators suggest that Iranian cyber capabilities may now even be closing on Russia[1183]. However, with the Belfer Centre's 2020 *Cyber Power Index* only placing Iran 20th in its overall standings and classifying it as a state with 'high intent but low capability', such predictions may be overstated[1184]. To explore this further and assert whether Iran can meet its intent and credibly threaten Western air power through the cyber domain, the discussion will next explore Iranian cyber capabilities.

Iranian Cyber Capabilities

If asked in early 2000 whether Iran has the cyber capabilities to target Western air power, whether that be Western industry, its public sector or the military, most analysts would have offered a very low assessment. However, this would change in 2014 when US firm Cylance published a report which alleged that since at least 2012 Iranian state-sponsored actors had 'directly attacked, established persistence in, and globally extracted highly sensitive materials' from Western governmental and commercial networks[1185]. Collectively naming the attacks Operation Cleaver and labelling Iran in cyber terms as 'the new China', Cylance succeeded in changing how the world viewed Iran as a cyber power[1186].

Though significant, Cylance further assessed that their visibility only represented a fraction of Iran's full cyber operations. Whilst further surveillance of Iran to discover more may have been tempting, Cylance decided that having witnessed Iran's capabilities rapidly evolve it had no choice other than to protect the interests

For Iranian increases in cyber spending, see:
Small Media, "Iranian Internet Infrastructure and Policy Report: Special Edition - the Rouhani Review (2013–15)", (2015), 6.

[1183] For the Alperovitch quote and assessment of Iran's growing cyber capability, see:
C. Bennett, "Fears Grow of Iran Cyber Attack", *The Hill* (2014).
For the IRGC cyber budget, see:
N. Bertrand, "Iran Is Building a Non-Nuclear Threat Faster Than Experts 'Would Have Ever Imagined'", *Insider* (2015).
For an assessment of Iran as a cyber power, see:
D. Kennedy, interview by N. Bertrandibid.

[1184] Voo et al., "National Cyber Power Index 2020", 11.

[1185] Cylance, "Op Cleaver ", (2014), 5.

[1186] Examples of Operation Cleaver being found in malicious software include in the namespaces of custom bot code codenamed TinyZBot and in Programme Databases (PDB) used by the group. For details see:
Ibid., 8.
For 'Iran is the new China' quote, see:
Ibid., 5.

of those being targeted by publishing their intelligence[1187]. Doing so through a comprehensive 85-page report, Cylance offered those defending target systems and networks Iranian Tactics, Techniques and Procedures (TTP) so that they could be countered[1188].

With the Cylance reporting also suggesting that Western intelligence agencies had been tracking this suspected Iranian state-sponsored cyber activity, its publication in 2014 quickly forced official bodies to also offer alerts. For example, in the week following the report the Federal Bureau of Investigation (FBI) issued a 'flash' warning to both commercial and public organisations[1189]. Offering further details on Iranian cyber TTPs, the FBI information was recognised by Stuart McClure, Cylance's Chief Executive, as 'underscoring Iran's determination and fixation on large-scale compromise of critical infrastructure'[1190].

Though this oversight confirms the development of Iranian cyber, to assess whether Iran is now capable of targeting Western military capabilities including air power it is necessary to consider in more depth the examples identified by Cylance alongside subsequent reporting. To begin, it is logical to consider one of the earliest known Iranian cyber attacks on a Western military capability, the 2011 hijacking of a US Sentinel UAV.

Reported to be operated by the CIA for surveillance purposes, the platform formed part of an increasingly well financed US drive to develop and field UAVs in all areas of operations. With this push receiving an uplift in funding from $2.3 billion in 2008 to $4.2 billion by 2012, UAVs became widely employed especially in reconnaissance roles[1191]. Though offering significant capability, Hatmann and Steup warned as early as 2013 that from a technical perspective 'UAVs must be classified as highly exposed, multiple linked, complex pieces of hardware with high strategic and economic value'[1192]. Continuing in their analysis, they further

[1187] Ibid., 8.

[1188] Ibid.

[1189] For a summary of the FBI 'flash' alert, see:
J. Finkle, "Exclusive: Iran Hackers May Target U.S. Energy, Defense Firms, Fbi Warns", *Reuters* 13 December 2014.

[1190] S. McClure, interview by Staff Writer, 13 December 2014.

[1191] L.C. Baldor, "Flashy Drone Strikes Raise Status of Remote Pilots", *Boston Globe*, 12 August 2012.

[1192] Hartmann and Steup, "The Vulnerability of Uavs to Cyber-Attacks; an Approach to the Risk Assessment".

noted that despite these factors, more research had at the time been conducted into the security of cars than into the security of UAVs[1193].

Exploiting this misbalance, Iran claimed on 4 December 2011 to have purposefully downed the CIA UAV. Broadcasting pictures on Iranian television, the apparently undamaged platform was being inspected by IRGC personnel including Brigadier General Amir-Ali Hajizadeh, Head of the IRGC Aerospace Unit, who claimed that his unit had successfully 'electronically hijacked' the UAV forcing it to land on an Iranian airfield[1194]. Exploring how Iran achieved this, Tyugu hypothesises that it was probably the digital link between the UAV and its land-based command and control element that was hacked. Once achieved, he suggests, 'wrong GPS data was likely passed to the control system' causing it to land on the Iranian airfield[1195]. Developing this in more depth, other cyber security bloggers have, through open-source analysis, suggested that the Russian Avtobaza jamming and electronic intelligence system was likely used to jam or spoof the data links. Though primarily used to target surveillance and fire control radars, it remains possible that the Avtobaza could have been repurposed by Iran[1196].

Regardless of the means through which the UAV was downed, the impact remains unchanged. Firstly, it proved as early as 2011 that Iran had the cyber capability to directly target Western air power, and a form of Western air power that states are increasingly reliant on. Secondly, though US authorities originally denied the loss, the situation ultimately forced US President Obama to acknowledge the situation asking Iran in December 2011 if they could 'please have their UAV back'[1197]. In doing so, Iran was handed a strategic victory by

[1193] Ibid.

[1194] A.S. Hashim, Patte, G. , "“What Is That Buzz?” the Rise of Drone Warfare", *Counter Terrorist Trends and Analysis* 4, no. 9 (2012).

[1195] E. Tyugu, "Command and Control of Cyber Weapons", in *4th International Conference on Cyber ConÀ ict* (Tallin 2012).

[1196] For open-source analysis of the likely means of downing the US UAV, see:
Unknown to Aviationintel.com, 2011, http://aviationintel.com/downed-rq-170-sentinel-drone-critical-updates/.
For further detail on the Avtobaza system, see:
Rosoboron Export, "Avtobaza-M Air Defence System ", (2022).

[1197] For reporting on the request to return the UAV, see:
E. MacAskill, "Obama Appeals to Iran to Return Downed Us Spy Drone", *The Guarian* 12 December 2011.
CNN, "Obama Says Us Has Asked Iran to Return Drone Aircraft".

openly proving that this regional power could, through cyber means, have direct impact on Western air power.

Though this impact caused UAV security measures to rise in national agendas, the reality of insecurities remains largely undiminished[1198]. Specifically, whilst the platforms continue to require datalinks to be operational, these datalinks will be susceptible to cyber attack. With no human pilot on board to identify and override such attacks and true autonomy through AI not yet realised, the platforms remain vulnerable[1199]. Therefore, with Iran having already experienced the advantage it can achieve by targeting Western UAVs, and with the West increasingly reliant on them to project power in the region, the likelihood of Iran using cyber to target air power in this way remains credible.

Looking beyond this direct threat, Iran has also shown the capability to target supporting systems and networks. Taking fuel supplies as an example, an Iranian cyber attack on Saudi Aramco in 2012 not only risked disrupting international oil supplies but also showcased an ability to target and impact well protected networks within an escalating cyber conflict[1200]. Referring to Iran's escalation in response to the 2010 Stuxnet attack, classified US documents leaked by Snowdon confirmed a Western intelligence assessment that the Saudi Aramco attacks were a clear retaliation. Not only this, but they further assessed that the impact of the attack in which data was destroyed on tens of thousands of computers showed 'a clear ability to learn from the capabilities and action of others'[1201].

With Iran conducting a similar attack against Qatari company RasGas, a trend appears in which Iran had, as early as 2012, an increasing cyber capability and intent[1202]. Though not directed at military targets this ability, if redirected against

[1198] For the increase in interest in UAV security, see:
J. Keller, "Iran–U.S. Rq-170 Incident Has Defense Industry Saying 'Never Again' to Unmanned Vehicle Hacking", *Military-Aerospace Electronics* (2016).

[1199] For depth on current development in UAV datalinks and AI, see:
C.R.S. Kumar, Sanket, M. , "Current Trends in Cyber Security for Drones " (paper presented at the International Carnahan Conference on Security Technology (ICCST) 2021).

[1200] Kennedy, "How Iran Would Wage Cyber War against the United States".

[1201] US, "Iran - Current Topics", ed. National Security Agency (NSA) (The Intercept 2015).

[1202] For an assessment of the RasGas cyber attack, see:
J. Leyden, "Mystery Virus Attack Blows Qatari Gas Giant Rasgas Offline", *The Register* (2012).

military systems, could be highly disruptive. For example, if the systems supporting air operations were effectively targeted and key information lost, air power would be significantly impacted, limiting effectiveness until recovery could be achieved. In considering the likelihood of this, one might argue that military systems should be more secure than those of Saudi Aramco or RasGas. However, a successful Iranian cyber attack on the US MCI in 2013 proves that this is not the case.

Introduced in 1999 in response to the increasing challenge of managing an ever-growing collection of disparate systems, the MCI consolidated over 6,000 individual Marine Corps networks[1203]. Though intended to allow enterprise management and enhance security, the networking of so many systems created a tempting target for attack[1204]. It is therefore unsurprising that this potential was realised in September 2013 with reporting indicating that a group working directly for Iran's government successfully infiltrated the MCI[1205]. Though no classified information is reported to have been exfiltrated, it nonetheless caused deep concern[1206]. Leading the USN to launch Operation Rolling Tide in late 2013, the first US cyber defensive operation to be given a name in the USN, it was found that despite robust technical security measures the Iranian means of conducting the attack focused on 'relatively unsophisticated' social engineering and subsequent technical exploitations[1207].

Reflecting on this, and taken in combination with the damage done in the Saudi Aramco attacks, the MCI breach proved that Iran has the capability to successfully infiltrate Western military systems[1208]. Though in response Ray Mabus, USN Secretary, lauded Operation Rolling Tide as 'the largest and most sophisticated network manoeuvre in USN history', the response does not limit the potential damage[1209]. Based on this, the example underlines the assessment that

[1203] Norton, "The U.S. Navy's Evolving Cyber/Cybersecurity Story", 22.
[1204] Ibid.
[1205] S. Soesanto, "The Evolution of Us Defense Strategy in Cyberspace (1988 – 2019)", *Cyber Defense Project, Center for Security Studies* (2019): 17.
[1206] J.E. Barns, "Us Says Iran Hacked Navy Computers", *The Wall Street Journal* 27 September 2012
[1207] S. Lyngaas, "Revisiting the Navy's Blueprint for Cyber Operations", *FCW,* (2015).
[1208] Ibid.
[1209] For the Mabus quote, see:
Ibid.

if targeted against air power's supporting systems the Iranians could cause significant operational disruption.

Though this Iranian cyber capability has been shown to disrupt air power directly and have the potential to do so indirectly, this is not the only way in which air power could be impacted. Rather, as the previous discussion on left-of-launch attacks attests, Iran could, by targeting the networks of supporting infrastructure such as fuels and power, have similar disruptive effects. Whilst no examples of such Iranian attacks on Western military infrastructure have been found, what is known is that Iran can do so if it chooses. This is illustrated by its 2013 attack on the sluice gate controls of a dam in New York, US.

Assessed by Kennedy as having the potential to be the first kinetic cyber attack in the US homeland, the attack according to US Justice Department documents may not have been sophisticated but still demonstrated Iranian capabilities[1210]. Naming the attackers as being linked to 2 groups associated with the Iranian state, US court papers alleged that between August and September 2013 the hackers obtained unauthorised remote access to the dam's SCADA system[1211].

Allowing them to gather information on water levels, temperature, and the status of the sluice gate, the access could, if the gate had not been disconnected for maintenance at the time of the attack, have allowed the group to flood the local area[1212]. Though not the most serious of potential outcomes, Dianne Feinstein, Vice-Chairperson of the US Senate Intelligence Committee, stated that it highlighted both the weaknesses in critical infrastructure and, importantly, the enormous damage that could be wrought if such Iranian state-actors successfully accessed 'the electrical grid, airports, water supply or nuclear plants'[1213].

[1210] For Kennedy's assessment, see:
Kennedy, "How Iran Would Wage Cyber War against the United States".
For the US Justice Departments documents, see:
K.E. Hemsley, Fisher, R.E., "History of Industrial Control System Cyber Incidents ", (US Department of Energy 2018), 13.

[1211] A. Hassanzadeh, Rasekh, A, Galelli, S. , "A Review of Cybersecurity Incidents in the Water Sector", *Journal of Environmental Engineering,* 146 (2020): 8.

[1212] Ibid.

[1213] D. Feinstein interview by J. Marks, 24 March 2016.

Extrapolating this out to networks that support air power including fuels and power which, like the dam in New York, are not controlled by the military, Feinstein's warnings resonate wider. With Iran demonstrating how it has the intent and capability to attack CNI in its adversaries' countries, there is a strong likelihood that it could redirect those abilities towards undermining the supporting air power infrastructure of an adversary.

In considering how this might be achieved and adding a further layer to the growing cyber capabilities of Iran, it is finally worth considering its alleged targeting of Western military personnel through cyber means. First reported in July 2021, Facebook announced that it had taken down approximately 200 fake accounts used by Iranian hackers[1214]. Believed to have been set up to target US, British and European military and defence personnel, the activity was assessed to be linked to a group known as Tortoiseshell. Identified by cyber security company Symantec, Tortoiseshell is thought to have used means including the Facebook sites and other fake military related recruitment websites to infect the computers of victims with malware[1215]. Once infected, the hackers stole login information and retrieved various information about the user and the system[1216].

Following a classic hostile actor route designed to facilitate further exploitation, the Meta Threat Intelligence Team assessed the activity as having all the 'hallmarks of a well-resourced and persistent operation' with clear ties to the Iranian state[1217]. An assessment supported by the assertion that the malware used by the group is known to have been developed by Mahak Rayan Afraz (MRA), an IT company based in Tehran with ties to the IRGC, the activity demonstrates a further facet to the Iranian cyber capability[1218].

Whilst concerning in isolation, this development also offers depth to the potential threat posed by Iran to Western air power. With the campaign directed solely at

[1214] N. Gleicher, "Iranian Hackers Targeted Western Militaries", *United States Peace Institute* (2021).
[1215] Threat Intelligence Team, "Tortoiseshell Group Targets It Providers in Saudi Arabia in Probable Supply Chain Attacks", (Symantec 2019).
[1216] A. Stoica, "Social Engineering as the New Deception Game", *Romanian Journal of Information Technology and Automatic Contr,* 31, no. 3 (2021): 61.
[1217] M. Dvilyanski, "Taking Action against Hackers in Iran", (Meta, 2021).
[1218] Ibid.

Western military personnel, it demonstrates a clear intent to access their information for further exploitation. Whilst such exploitation may range from subversion to laying the groundwork for future social engineering, the end point for a sophisticated state-sponsored actor is likely to be the same: to gain the information necessary to access military systems and networks. With such networks including those supporting air power, and the MCI attack showing that Iran has achieved this in the past, the picture grows to one in which Iran is a capable cyber actor willing to use direct, indirect, and left-of-launch means to access its adversaries' networks for hostile reasons. Based on this, it can be concluded that though not in the same class as the PRC or Russia, Iran remains a growing cyber power with the potential in times of heightened tensions or conflict to target and disrupt Western air power through cyber means.

Conclusions on the Iranian Threat to Western Air Power

Concluding the examination of the three cyber threats to Western air power, this section discussed Iran. Initially summarising the steep decline in relations with the West since the 1970s and the ensuing ideological struggles for regional control, the roles of Iranian cyber capabilities and Western air power in this context were explored. Noting that if tensions overflowed to conflict Iran is likely to fight in an asymmetric way, cyber was identified as increasingly central. As it was also noted that Iran views Western air power as a key factor that must be blunted if conflict were to arise, the importance of charting the development of Iran as a cyber power was identified. Ranging from direct to left-of-launch threats, the discussion concluded that Iran continues to be a state with growing cyber capabilities which has the potential to disrupt Western air power.

It is evident therefore that the Iranian cyber threat is not as credible as those posed by either the PRC or Russia. However, its pace of development is identified as offering a motivation for Iran to pursue its regional agenda. Potentially able to harass and disrupt Western air power, the use of cyber attacks, even if any impact were quickly overcome, may embolden Iran. If this occurs, events may reinforce Iran's hard-line leadership and shift strategic calculations in the Middle East. It can therefore be concluded that whilst the Iranian cyber threat to Western air power may not be significant, it remains in the context of regional tensions a notable concern.

Conclusion

Taking a representative constructivist cross section of the PRC as a superpower in waiting, Russia as a great power pushing to maintain global relevancy and Iran as a regional power seeking to assure operational influence, the section explored potential cyber threats to Western air power. Opening with the PRC, an overview of Western-Sino relations noted that despite a period of promise in the 1990s, fracture lines driven by fundamental differences in governance, economic practices, and human rights formed a clash that is likely to 'shape geopolitics for decades'[1219].

Examining whether the PRC's cyber capabilities would be decisive in such a clash, and the threat to Western air power within this, the nature and its underpinning cyber capabilities were discussed. In the first area, the PRC's use of cyber was identified as supporting its wider grey zone intent by disrupting military capabilities including air power, achieving advantage, and preventing conflict before it has begun. In a second area, it was further noted that this intent could now be viably achieved through credible cyber capabilities that have been proven as able to deter and threaten Western air power.

Reviewed in a concluding section, it was noted that cyber will likely play a key role in both the PRC's path to and conduct of a potential Sino-Western conflict. Including in this a necessary disruption of Western air power, the assertion underlined the overall narrative of the PRC pursuing a form of grey zone conflict intended to achieve its cyber supported strategic goals without resorting to armed conflict.

[1219] Jones, "Global China: Assessing China's Growing Role in the World."

Turning next to Russia, a great power striving to maintain global relevance, its relations with the West, that have been tested through NATO’s eastward expansion, were explored as a means of asking whether Russia poses a credible cyber threat to Western air power. Initially considered through a discussion on the nature of the Russian cyber threat, the state was identified as one of the greatest concerns to Western interests with cyber forming an anchoring capability within this. Developed further through an examination of Russian cyber capabilities, examples of its activities were shown to illustrate how Russia has reached a point at which it poses a credible cyber threat to Western air power.

In reviewing this discussion, the importance of Western air power in deterring Russian military aggression against NATO members was identified. With Russia shown to have the intent and, via both direct and left-of-launch capabilities, the means to disrupt air power, it was concluded that assuring the cyber defence of Western air power assets was a keystone to assuring the security of Western states in Russia’s near abroad.

Concluding the examination of the representative cyber threats to Western air power, the regional power of Iran was discussed. Initially summarising the downward trajectory of Western-Iranian relations from 1979 onward, it was acknowledged that the two sides continue to be locked in an ideological battle for regional control. To understand what role cyber may play in this battle, the nature and capability of Iranian cyber means were also explored.

In summary, it was ultimately asserted that Iran does not pose as credible a threat to Western air power as either the PRC or Russia. Notwithstanding this, it was further asserted that Iran could through a combination of cyber and conventional capabilities achieve short-term operational advantage which may embolden Iran’s hard-line leadership and shift the regional strategic balance. Given the seriousness of such a shift for Western interests, it was finally concluded that the West and its regional allies would be advised to closely follow and be prepared to defend against Iranian cyber threats to air power.

Reflecting on these discussions of the PRC, Russia, and Iran, a cohesive but complex picture is presented. In terms of its cohesiveness, all demonstrate that whether operating against a near superpower, a great power or a regional power, cyber means have a credible likelihood of disrupting operations. With air power also shown to be keystone to Western operations against all three, and cyber means specifically illustrated as able to disrupt such air power, a broad and credible cyber threat to Western air power is identified.

What complicates this conclusion is the complexity of the issue. Firstly, though all present a threat, the threats are distinct. For the PRC, the cyber threat is long-term. Intended to gain strategic advantage through cyber means, it is likely that if this cyber threat is not combatted the PRC will successfully deter Western air power and pursue its expansionist agenda. With this potentially occurring before the full extent of such expansionism is realised, the West must act now to secure its relative technological advantages and subsequent freedom of manoeuvre.

Alternatively, for Russia, the cyber threat is more immediate. Intrinsically tied to conventional means to achieve strategic intent, the West must be prepared to identify and counter threats as they occur. The West must also be clear on where aligned cyber activity not only breaches thresholds but signals further coordinated activity. If this is not achieved successfully, the West may be progressively pushed back in the tide of an aggressive Russia seeking regional dominance.

Finally turning to Iran, the threat may be much less direct but has the potential to strategically unbalance the region. Likely achieved using cyber in coordination with conventional means to achieve operational impact against Western air power, such actions could embolden the Iranian leadership. In doing so cyber means may prove decisive in pushing forward Iran’s regional aspirations and unbalancing the strategic situation in the Middle East.

Given these conclusions, it can be asserted that the cyber threat to Western air power is backed by distinctively individual but collectively credible intents to employ cyber means to achieve strategic advantage. With such intent firmly underpinned by varying but credible cyber capabilities, there is little doubt that on all fronts the West faces a concerning cyber threat to its keystone air power capabilities.

Chapter 9: Assessing the Cyber Risk to Western Air Power (Case Studies)

Introduction

Having introduced the research in Part 1, the second Part of this thesis established the importance of air power as a keystone capability to maintaining Western strategic advantage. Expanding this discussion to cyber risk, it was further established how the loss or compromise of air power through digital means could threaten the contemporary role of states. To test this assertion, this third Part has focused on the cyber risk to Western air power by examining its constituent parts of cyber vulnerabilities and cyber threats through three representative states in each area.

Opening with Western air power’s cyber vulnerabilities, examples of the US as a superpower, the UK as a residual great power and Taiwan as a Western-aligned regional power were explored. Through this, it was established that credible cyber vulnerabilities exist in the air power of all which, if exploited, could negatively affect all states. Within this, it was further assessed that the potential impact of cyber vulnerabilities is likely inverse to size, with the impact on smaller states more significant than those with greater resources. However, it was finally acknowledged that such vulnerabilities are only of concern if targeted by hostile actors with the intent and capability to exploit them.

To explore this assertion, the cyber threat to Western air power was considered. Examined through the representative examples of the PRC, Russia, and Iran, the threat from each was found to be distinct in nature and form. Despite these variables, all were concluded as having both viable cyber capabilities and the intent to target, disrupt and undermine the strategic viability of Western air power.

Through these discussions, the thesis has established that Western air power exhibits concerns in both the vulnerability and threat elements of cyber risk. With it also shown that the impact may vary depending on the state, it has been proven that cyber risk could undermine the West's strategic advantage but that such impact is relative, not absolute.

Whilst this assessment in isolation endorses the thesis' assertions on the concerns surrounding the cyber risk to air power, it is finally necessary to confirm the assessment and degree of variation through three representative scenario-based case studies. To do so, this Chapter will draw in each of the states examined above by considering the possibility of a PRC attack on Taiwan, a Russian attack on the Baltic States and, finally, a clash between Iran and Western aligned states in the Strait of Hormuz. Having presented these it will be concluded that the above assertions are correct. Notably, air power is a vital strategic capability which is susceptible to loss or compromise because of cyber risk. However, as asserted, the impact of this is also relative, not absolute, with the ultimate level of concern inverse to the size and resource of the state.

The Taiwanese Question

Located 100 miles off the PRC's southeast coast, the island of Taiwan with a population of 23 million is at 36,000 square kilometres roughly the size of Belgium[1220]. Though dwarfed by its neighbour, the emergence of this fiercely independent island that is faced by an existential PRC threat but supported by the US has led it to emerge as more geopolitically important than its size suggests.

In terms of potential conflict between the PRC and Taiwan, the calculus focuses on a fine balance. Within this, key elements are the Taiwanese military with significant but less exquisite military capabilities, a US with large capabilities which under strategic ambiguity may or may not be deployed, and a PRC whose pursuit of a 'great rejuvenation' has allowed its military to improve at pace[1221]. With this PRC capability augmented by growing non-conventional strengths,

[1220] Textor, "Taiwan - Statistics and Facts ".
[1221] US, "Military and Security Developments Involving the People's Republic of China - Annual Report to Congress", iii.

some argue that the likelihood of the PRC militarily reclaiming Taiwan 'is much closer than most think'[1222].

To achieve such an invasion, however, the PRC must cross the 100 miles of open water. To do so, air superiority is essential if it is to ensure the effective landing of troops[1223]. Though even without the US the Taiwanese in the early 2000s outmatched PRC's regional air power, developments in quality and quantity of aircraft had by 2019 pushed the balance in the PRC's favour[1224]. Through this advancement the PRC might be expected to easily achieve the necessary air superiority.

However, with Taiwan maintaining a large number of fighters including the largest F-16 fleet in Asia, it could in isolation inflict significant damage on an attacking force[1225]. When added to routine deployments of US air power to the region, the balance of power, assuming the US would intervene, shifts back to a level at which the PRC cannot guarantee air superiority[1226]. Reflecting on this, the question is whether the PRC's growing cyber power could, through its direction against opposing air power, be the factor which tips the balance in the PRC's favour and emboldens it to militarily enforce the 2015 Anti-Secession Law.

Considering this, the first point to address is the closing gap between PRC and Western air power. Though the balance remains in the US-Taiwanese favour, this advantage is increased through the fact that some key PRC technology remains behind that of the West. For example, the new J-20 W-15 engine is reported to be unable to handle high temperatures. This means that PRC air power without

[1222] For a summary of the interplay between the PRC and Russian intent, see:
Wong, "China: What Does It Want from the Ukraine Crisis with Russia?".
For the quote, see:
Aquilino, "China Threat to Invade Taiwan Is 'Closer Than Most Think', Says Us Admira."

[1223] For the importance of air power in a PRC invasion of Taiwan, see the scenario presented in:
Lague, "T-Day: The Battle for Taiwan ".

[1224] Joe, "Anatomy of a Taiwan Invasion: The Air Domain".

[1225] Details on the size of the Taiwanese Air Force differs depending on the source. Estimates range from approximately 300 to 400 4th generation fighters. Representative sources include:
Ibid.
Global Firepower, "2022 Taiwan Military Strength ", (Global Firepower 2022).

[1226] For USN carrier deployments to the region, see:
B. Blanchard, "U.S. Carriers in South China Sea, Taiwan Reports Further Chinese Incursion", *Reuters* 24 January 2022.

improvements remains incapable of performing on a par with Western cutting-edge platforms[1227].

In addressing this it is assessed as likely that the PRC will continue to pursue its cyber espionage campaign. This was illustrated by the 2021 US conviction of a senior Chinese Intelligence Officer. Proved to be attempting to steal secrets on military jet engines via cyber means from US company General Electric, the case confirms that the PRC is actively attempting to resolve its known capability gaps[1228]. Having done so in the past to great effect, one can envision a point at which the large PLAAF has delivered platforms whose limitations have been rectified. At this point, the PRC's long-term cyber exploitation of the grey zone would be credited with shifting the PRC-Taiwanese balance of power through air superiority to a point at which it can be certain of militarily reclaiming the island.

Moving closer to conflict itself, the PRC's employment of its CNI focused left-of-launch capabilities could also viably play a part in achieving air superiority by degrading its adversary's air power. Though achievable via kinetic strikes, a viable option that would not destroy the valuable Taiwanese industrial base would be cyber attacks against the island's CNI.

Addressing the viability of this threat Yang Wei-fuu, Chairman of the state-owned Taiwan Power Company (Taipower), confirmed in 2021 that his company had 'encountered cyber attacks almost every day'[1229]. Though no damage has to date been reported, Chien Hung-wei, Head of Taiwan's Department of Cyber Security, also asserted in 2021 that the island has been subject to 'tens of millions of attacks monthly'[1230]. Whilst not all are attributed to the PRC, Hung-wei identified a series of ransomware attacks in 2020 against 10

[1227] Z. Keck, "Engine Problems: Why China's J-20 Stealth Fighter Can't Beat America's F-22 or F-35", *The National Interest,* (2020).

[1228] For arguments that information alone will not help the PRC, see:
Farley, "Theft Can't Help China's Air Force Build Quality Engines".
For the conviction of a PRC Intelligence Officer, see:
D. Sevastopulo, "Chinese Intelligence Officer Convicted of Stealing Secrets from Ge", *Financial Times* 5 November 2021.
For General Electric's role in military engine design, see:
General Electric, "Military Engines ", (2022).

[1229] H. Tzu-ti, "Taiwan's National Power Company Hit by Cyberattacks on Daily Basis", *Taiman News*, 6 December 2021 2021.

[1230] Ibid.

Taiwanese CNI providers that were confirmed as originating from PRC state-sponsored hackers[1231].

Introducing a self-propagating malware through a backdoor, these attacks caused networks to crash and prevented access to payment systems[1232]. Identified as part of a wider pattern of PRC attempts to probe and map Taiwanese CNI, Yun Sun, co-director of the East Asia programme at the Stimson Centre, warns that they are likely to have offered the PRC the ability to shut down Taiwanese CNI at will in the event of conflict. Though he concedes that such attacks would not disable Taiwan's defence system, he does assess that they would have significant impact[1233]. When placed in the context of air power, which compared to the other domains has a heightened reliance on CNI, such activity could disrupt operations to a point at which the PRC is handed decisive advantage in the achievement of air superiority and the subsequent invasion of Taiwan.

Continuing in this left-of-launch theme, but taking a more oblique position, such CNI attacks could also be used against other Western adversaries likely to support Taiwan in the event of conflict. Taking attacks on US ONG infrastructure as an example, such action may not disrupt military capabilities in the Asia-Pacific but may undermine political will and public support for defending Taiwan. Specifically, by confirming the impact the PRC could have through cyber means on those supporting Taiwan, they may shift the cost-balance discussion to a point at which the West withdraws its forces. Including the withdrawal of air power, the scenario reinforces how cyber means employed via the 'Chinese way' in grey zone conflict could have a wide-ranging impact on the Taiwanese question.

Turning to a final left-of-launch vector, disruption of space-based assets, a further PRC cyber capability is identified that could have a major impact on the West and Taiwan's ability to employ air power to deter or prevent a military attack. Referring

[1231] Chien Hung-wei, interview by E. Cheung, Ripley, W.. Tsai, G. , 24 July, 2021.
[1232] Staff Writer, 2 June, 2021, https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5.
[1233] Y. Sun, interview by R. Jennings, 10 December 2021.

to the unparalleled reliance of air power on space-based assets which range from communications, through navigation to the means of delivering PGMs, the reality is that an effective disruption of Western space capabilities would degrade if not prevent its use of air power[1234].

The ability of the PRC to direct such counter-space capabilities against the West and its allies were underlined by a 2017 US Congressional report which stated that it already had 'the engineering and expertise…to develop counter space cyber weapons'[1235]. Underlined by known PRC cyber actions including the 2007 attack on the US Geological Survey's Lundsat satellite and the 2014 attack on the NASA Terra Earth observation satellite, there is little doubt that the PRC could adopt this left-of-launch vector to disrupt Western and Taiwanese air power[1236]. If conducted during a crisis, such activity may not be the only factor in whether the PRC is successful but could still offer a decisive edge. In such circumstances, a further example is offered of how grey zone conflict delivered in the 'Chinese way' can achieve political aims without kinetic exchanges.

Considering this case study, it is evident how cyber is likely to play a key role in both the path to and conduct of any potential conflict with Taiwan, including in the PRC's necessary disruption of Western and Taiwanese air power. Within this, however, there is a possibility that such predictions may never be seen. With the PRC signalling its cyber capabilities as part of a deterrence strategy, the mere threat of cyber debilitating key capabilities, including air powers supporting infrastructure, may convince the West and Taiwan that any attempt at defence is unviable. In such circumstances, the case study may act as the ultimate proof that the PRC's approach to grey zone conflict forms an ideal blueprint for a rising power to achieve its strategic intent through cyber means without resorting to armed conflict.

[1234] For depth on air power's reliance on space-based assets, see:
EMEA, "Aviation: Satellite Services".
For depth on PGM's reliance on space-based assets, see:
Perju, "Precision Guided Bombs: Analysis", 112.

[1235] Chen, "Opening Statement of Mr David D. Chen Independent Analyst: Hearing before the Us China Economic and Security Review", 75.

[1236] For depth on the 2007 cyber attack on the US Geological Survey's Lundsat satellite, see:
Ibid.
For depth on the 2014 cyber attack NASA Terra Earth observation satellite, see:
Harrison, Johnson, and Roberts, "Space Threat Assessment 2018", 13.

Reflecting on this conclusion, the cyber risk to Western air power is through the Taiwanese question not simply proven but shown to have depth. Notably, on one level, it has illustrated how US and Taiwanese air power exhibit direct and indirect cyber vulnerabilities. With the PRC also shown to have the capabilities and intent to form a credible cyber threat, a cyber risk to air power emerges. With air power pivotal to any PRC attempt to take control of Taiwan by force, this cyber risk to air power could, if realised, undermine Western strategic advantage during any conflict in the Asia-Pacific.

On a second level, the case study also shows how the mere potential of cyber risk being realised may be enough to prevent US involvement in a crisis. In such circumstances, the cyber risk to Western air power becomes such a potent deterrence for the PRC that it can achieve its aims without ever having to employ its cyber capabilities. Through this a position is reached in which the cyber threat does not even need to be real, and the PRC does not even need to achieve through cyber means what it has been suggested it can. Able to undermine and remove the strategic capability of Western air power through the deterrence effect alone, cyber risk reaches the level of importance exhibited by other capabilities such as the nuclear deterrent. In this context, the cyber risk to Western air power becomes recognised as a defining feature of the modern strategic calculus.

The Baltic States and NATO's Eastern Frontier

The Baltic states of Estonia, Latvia and Lithuania offer an informative case study when considering Russian militarisation of cyber to target Western air power. Following the collapse of the Soviet Union, the military capability of the Baltic states was limited. Though the apparent benefits of the post-Cold War 'peace dividend' suggested that such limitations were unimportant, the Baltics political leadership saw the situation very differently. With the Estonian Foreign Ministry commenting in 1993 that 'the most important lesson is simple: time is short, and time will not wait for small nations'[1237], their intent to move closer to the West before Russia could regain a stronger position was set. Working to do so throughout the 1990s, the Baltic states achieved NATO and EU membership in 2004[1238].

Such Western alignment of states on its borders would, in the late 1990s, elicit a strong reaction from a Russia attempting to regain control in its traditional sphere of influence. Summarised by Sergey Lavrov, Russian Foreign Minister, this reality saw Russia leave the path 'our Western partners had tried to make [us] follow' and embark on its own path which has included coercion of neighbouring states[1239]*.*

For the Baltics, this created uncomfortable uncertainties. Though not yet subject to military incursions, Russia has maintained clear strategic goals to reverse Baltic alignment with the West which it views as an 'inherent threat to its security'[1240]. To do so, the Russian intent is threefold: prevent increased NATO presence in the Baltics, develop and maintain control of critical infrastructure in the region, and counter the narrative that characterises the Soviets as occupiers[1241]. With large Russian-speaking communities also residing in the Baltic states, and the defence of similar communities invoked by Russia as justification for other conflicts, there is a credible risk that Russia could use force to enter and exert control over at least portions of the region[1242].

Exploring this threat, Russia had before the Ukraine conflict concentrated its best trained troops in the Western Military District (WMD) that borders the Baltic region. Estimated to number approximately 30,000 personnel in 2021, it is

[1237] For the quote, see:
Unknown, "Estonian Foreign Ministry Memo," in *The Baltic States and the End of the Cold War*, ed. K. Piirimäe, Mertelsmann, O. (Berlin: Peter Lang, 1993).
For depth on the 'peace dividend', see:
H. Davoodi, Clements, B., Schiff, J., Debaere, P., "Military Spending, the Pease Dividend, and Fiscal Adjustment", *IMF Staff Papers* 48, no. 2 (2001): 291.

[1238] A. Banka, "The Breakaways: A Retrospective on the Baltic Road to Nato", *War on the Rocks* (2019).

[1239] S Lavrov, interview by Russian News Agency, 28 October 2014.

[1240] E. Lucas, Hodges, B., Schmiedl, C. , "Close to the Wind: What Russia Wants", *Center for European Policy Analysis,* (2021).

[1241] Ibid.

[1242] For depth on the Russian threat to the Baltic states, see:
U. Bergmane, "'Fading Russian Influence in the Baltic States", *Orbis,* 64, no. 3 (2020).

acknowledged that since mid-2022 Moscow has progressively moved forces away to augment high losses in Ukraine[1243]. In the estimate of some sources, this could be as significant as an 80 percent reduction of troops in the WMD[1244].

This might indicate a permanent reduction in the Russian threat to the Baltics. However, regional leaders disagree. For example, whilst Russian Army numbers may have reduced, Finnish Defence sources report that Russian air and naval power has not changed in the region[1245]. Furthermore, despite heavy Russian losses in Ukraine, Kusti Salm, the Permanent Secretary to the Estonian Ministry of Defence, predicted in June 2022 that given the regions geopolitical importance Moscow will inevitably 'come back stronger'[1246].

Explored in the context of NATO strategy, Kaja Kallas, the Estonian Prime Minister, also cautioned against the current Alliance stance 'to lose it and liberate it afterwards'[1247]. This describes the NATO position which hopes its tripwire deters but, in the event of aggression, would allow the Baltics to be overrun before planning to liberate them after 180-days.

In response to these public comments, Jens Stoltenberg, Secretary General of NATO, indicated a change to NATO policy ahead of the 2022 Madrid Summit. This was further underlined after the summit with the Allies outlining a New Force Model which should see 300,000 troops held at high readiness to respond to attacks on NATO members, and reinforced stockpiles forward mounted in the Baltics. However, with these developments merely enhancing the current posture, and no clear statement on NATO formally changing its Baltic strategy,

[1243] For WMD standing forces, see:
A.M Dyner, "Russia Beefs up Military Potential in the County's Western Areas", *The Polish Institute of International Affairs* (2019).
For exercise surges, see:
K. Muzyka, "Russia Goes to War: Exercises, Signalling, War Scare and Military Confrontations", *Centre for Strategic and International Studies,* (2021).

[1244] For the Finnish Defence Command statement, see:
R. Gramer, "Russia's Stripped Its Western Borders to Feed the Fight in Ukraine", *Foreign Policy*, 28 September 2022.

[1245] For the Finnish Defence Command statement, see:
Ibid.

[1246] K. Salm, interview by J. Grady, 16 June, 2022.

[1247] K. Kallas, interview by R. Milne, 22 June, 2022.

both regional leaders and Russia can assume that the 180-day intent remains an underlying NATO planning assumption[1248].

Given this, Kallas's criticisms reflect real fears of an existential threat to the Baltics. Put in graphic terms by citing Russian atrocities in Ukraine, she asserts that the 180-day strategy is not only untenable but would result in Estonia being 'wiped off the map and the historic centre of its capital city razed to the ground'[1249]. Made starker still by Russia's increasing warnings to the West of its potential use of nuclear weapons, especially in response to a NATO attack, a scenario can be envisaged in which Russia overruns the Baltics and a potential NATO counterattack is deterred. If this were to occur, a permanent loss of the Baltics to Russian control could be realised[1250].

Exploring the likelihood of such Russian aggression, other regional commentators note that Russia is not only likely to reconstitute its strength in the WMD but is even more likely to do so if the Ukraine campaign is in part successful. Making this argument in September 2022, Jonatan Vseviov, Secretary-General of the Estonian Ministry of Foreign Affairs, commented that Russia 'threw almost everything they had at Ukraine…[but to say that diminishes the threat to the Baltics]…is a very narrow way of analysing threat'. Expanding on this, he concluded that Russia remains 'extremely dangerous' with the nation becoming an increasing not diminishing threat to the Baltics if it 'at least partially achieves something they are after in Ukraine'[1251].

In response, NATO leaders as illustrated by the 2022 Madrid Summit have recognised that the Baltics represent 'something geopolitically bigger' than is

[1248] For Stoltenberg's comments, see:
J. Stoltenberg, interview by S. Meredith, 2022.
For changes to the NATO posture on its northern flank following the 2022 Madrid Summit, see:
NATO, "Nato Strategic Concept", (2022).
"New Nato Force Model ", (2022).

[1249] Kallas, "Estonia's Pm Says Country Would Be 'Wiped from Map' under Existing Nato Plans."

[1250] Examples of reporting highlighting Russian rhetoric on its potential use of nuclear weapons include:
P. Sauer, "Putin Flirts Again with Grim Prospect of Nuclear War – This Time He Might Mean It", *The Guardian*, 21 September 2022.
A. Davies, "Putin: Nuclear Risk Is Rising, but We Are Not Mad", *BBC News*, 7 December 2022.

[1251] For Vsevivo's quote, see:
Staff-Writer, "Russia Moved 80% of Troops from Nato Borders to Ukraine".

experienced elsewhere[1252]. Reflected not only in initiatives such as the New Force Model, other key developments include the creation of the Joint Expeditionary Force (JEF) and the extension of NATO membership to Finland and Sweden[1253]. Through these, it is evident that the West takes potential Russian aggression against the Baltics and the wider region seriously. If, however, this is to be translated into tangible action, four key issues must be addressed[1254].

Firstly, the Baltics are geographically isolated from the majority of NATO. With Russia and Belarus to the south and east, and with only one state, Lithuania, sharing a land border with another non-Baltic NATO state, Poland, the logistics of militarily securing the region are challenging[1255].

Secondly, the size of the Baltic states in population and geography means that if attacked they may be overrun before even the enhanced high readiness troops from elsewhere in NATO can respond. Though it is accepted that the experience in Ukraine has shifted this calculus, a series of RAND wargames in 2016 assessed that the longest it might take Russian forces to reach the outskirts of the Estonian and Latvian capitals was 60 hours. This would be far too short a time for NATO to offer meaningful reinforcements moving the discussion back to the 180-day strategy for recovery and the issues this involves[1256].

Thirdly, given the proximity to Russia, the entire area falls within Russian A2AD capabilities. This makes it difficult for NATO to achieve the level of air or maritime

[1252] L. Coffey, Kochis, D., "Nato Summit 2021: Reinforcing Collective Defence in the Baltics", *The Heritage Foundation,* (2021).

[1253] JEF is a UK led political forum with military underpinnings which provides a framework for the defence of Nordic and Baltic countries not all of whom are currently NATO members. For depth on JEF, see:
J. Wharton, "What Is the Joint Expeditionary Force?", *Forces.net*, 14 March 2022.
S. Monaghan, "The Joint Expeditionary Force: Global Britain in Northern Europe?", *Center for Strategic and International Studies (CSIS),* (2022).
For depth on Finland and Sweden joining NATO, see:
Staff-Writer, "When Will Sweden and Finland Join Nato? Tracking the Ratification Process across the Alliance", *Atlantic Council,* (2022).
J. Posaner, "'Hand-in-Hand': Finland, Sweden Pledge to Join Nato Together", 29 October 2022.
For comment on how seriously NATO take the Russian threat to the Baltics, see:
Coffey, "Nato Summit 2021: Reinforcing Collective Defence in the Baltics".

[1254] For the concept of 'cross-domain coercion', see:
D. Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy", *Proliferation Papers,* 54 (2015).

[1255] A. Hyde-Price, "Nato and the Baltic Sea Region ", *NATO Research Fellowship* (2000): 23.

[1256] Shlapak and Johnson, *Reinforcing Deterrence on Nato's Eastern Flank: Wargaming the Defense of the Baltics*, 1.

superiority that would be necessary to assure access without considerable military losses in a time of crisis[1257].

Finally, as noted above, the increased threat of Russian use of nuclear weapons in response to a NATO attack changes the calculus. This is because, if the Baltics were already under Russian control, the risk of NATO counter attacking as planned reaches another level of impact which the Alliance may not be willing to risk.

Exploring the best way for NATO to overcome these challenges and effectively defend the Baltics, Chang argues that the Alliance must make sure an attack never manifests itself by 'convincing Russia that it could not achieve a quick victory in the region'[1258]. To achieve this, twin factors are required: a credible political will to defend the Baltics and a credible military capability through which to deliver this will.

On the first issue of political will, Western leaders have never wavered. For example, speaking in 2014, German Chancellor Angela Merkel stated in response to questions over whether NATO would defend the Baltics that Article 5 'is not something which exists on paper, but which is filled with life…[meaning that] NATO will help straight away' if the Baltics were threatened[1259].

On the second issue of capability, the central element of the current NATO force in the Baltics was agreed at the 2016 NATO Warsaw Summit. Referred to as the Advanced Forward Presence (AFP), this consists of 4,000 NATO troops comprised of four multinational battalion-size battlegroups provided on a rotational basis by a mix of member states[1260]. Meant to offer a credible deterrence to Russian aggression, be an upgrade to the 2014 Wales Summit's 'mobile tripwire' and be further upgraded by the 2022 Madrid Summits New Force

[1257] For depth on Russian A2AD in the Baltics, see:
R. Dalsjö, Berglund, C., Jonsson, M. , "Bursting the Bubble: Russian A2/Ad in the Baltic Sea Region", *Swedish Total Defence Research Institute* (2019).

[1258] F.K. Chang, "Nato's Baltic Defence Challenge", *Foreign Policy Research Institute,* (2017).

[1259] A. Merkel, interview by Reuters Staff, 18 August, 2014.

[1260] NATO, "Boosting Nato's Presence in the East and Southeast", ed. NATO Newsroom (2022).

Model[1261], the AFP has been heralded as an 'unambiguous demonstration' of NATO's determination to defend the Baltics[1262].

Despite these commitments, the NATO strategy remains the questionable tripwire the Estonian Prime Minister has referred to [1263]. However, when supported by NATO air power assuring not only aerial sovereignty through the Baltic Air Policing mission, but also intelligence and assured access through additional NATO air platforms based elsewhere in Europe, NATO transforms the tripwire into something that credibly backs its political will to defend the Baltics. In doing so, air power becomes keystone to convincing Russia that a quick victory will not be possible which, in turn, deters Russia from the path of increasing influence over the Baltics through military means[1264].

With Russia equally aware of the importance of NATO air power, the key question that emerges is how, within its strategy of cross-domain coercion, could Russia undermine NATO air power to a point at which it is no longer a strategic deterrence? One likely answer to this question is for Russia to target NATO air power using cyber capabilities which, as explored above, remain a distinct possibility despite its underwhelming cyber performance in the Ukraine conflict.

Considered from an indirect cyber perspective, and reflecting on previous discussions within this thesis, the example of Operation Orchard provides one means through which Russia could achieve this. Referring to the Israeli disruption of Syrian air defences' which allowed the IAF to attack targets in Syria unscathed,

[1261] M. Zapfe, "Deterrence from the Groups Up: Understanding Nato's Enhanced Froward Presence", *Survival* 59, no. 3 (2017): 148.

[1262] NATO, "Warsaw Summit Communiqué", ed. NATO Press Release (2016).

[1263] For the concept of 'cross-domain coercion', see:
Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy".
For the Estonian Prime Ministers comments on the NATO tripwire, see:
Kallas, "Estonia's Pm Says Country Would Be 'Wiped from Map' under Existing Nato Plans."

[1264] For Chang's analysis, see:
Chang, "Nato's Baltic Defence Challenge".
For operational detail on how NATO air power would deter Russian military aggression in the Baltics, see:
R.M. Klein, Lundqvist, S.. Pettersson, U. , "Baltics Left of Bang: The Role of Nato with Partners in Denial-Based Deterrence", *Strategic Forum,* (2019): 11.
C. Harper, Lawrence, T., Sakkov, S., "Air Defence of the Baltic States", *International Centre for Defence and Security,* (2018): 21.
E. Cieslak, "Air Defence of the Baltic States: Looking toward the Future", *Safety and Defence,* 7, no. 2 (2021).
C. Rein, "Nato Air Deployments to the Baltics as Strategic Messaging," in *The Challenge to Nato: Global Security and the Atlantic Alliance* ed. M.O. David Slobodchikoff, G.D., Stewart, B. (Washington D.C.: Libary of Congress, 2021), 89.

similar tactics could be pursued by Russia[1265]. Though the regional Baltic Air Defence Network (BALTNET) and associated NATO air defences are more advanced than the exploited Syrian system, the thesis' discussion on left-of-launch attacks illustrated how even the most well protected networks remain vulnerable to cyber attack.

For example, in designing the type of secure digital environments one would expect NATO air defence systems to operate, architects routinely include means such as air gaps and data diodes[1266]. Preventing digital pathways into the system, these should logically avoid a cyber attack. However, with this assertion infamously shown to be incorrect by the Stuxnet virus, it proves that no matter how secure a network is it can never be fully protected[1267]. If this logic is applied to Russian targeting of NATO air defence systems, a possibility is evident in which Russia could cause the same level of air defence blackout over the Baltics as Israel achieved over Syria. In such circumstances, Russian air power could enter Baltic airspace undetected and through kinetic effects diminish NATO air power before it was able to react.

Beyond this example, further consideration of the left-of-launch concept identifies numerous other options for Russia to target NATO air power. Russia could, for example, decisively target NATO air power in any one of the three left-of-launch areas that have previously been explored: the supply chain, space, or infrastructure. Of these, infrastructure is, given Russia's previous cyber attacks on Ukraine, arguably the most likely. Within this, there is a credible risk that cyber attacks on infrastructure supporting NATO air bases both in the Baltics and wider Europe could be synchronised with a conventional Russian attack on the Baltics. If successful through the disruption of services ranging from power supplies to fuels, NATO aircraft could either be grounded or prevented from refuelling,

[1265] For details on Operation Orchard, see:
Kapan, "Air Power's Visual Legacy: Operation Orchard and Aerial Reconnaissance Imagery as Resus De Geurre".
Ibid., 61.
Horschig, "Cyber-Weapons in Nuclear Counter-Proliferation", 358.

[1266] Techopedia, "Air Gap ".

[1267] For depth on Stuxnet, see:
Sembiring, "Stuxnet Threat Analysis in Scada (Supervisory Control and Data Acquisition) and Plc (Programmable Logic Controller) Systems", 97.

rearming, and returning to combat. In either circumstance, Russia would be handed a decisive advantage.

A further left-of-launch area Russia could credibly target are supply chains. With numerous ransomware attacks from NotPeya to Bad Rabbit known to have originated from Russian state-sponsored sources, and this form of malware able to disrupt systems and networks, it is plausible that the NATO air power supply chain could be targeted through such cyber means.

Taking the F-35 as an example, the aircraft is now considered a strategically decisive air asset by the fifteen states which operate it, including the NATO members of the US, UK, Italy, and Germany. Though one might expect such an important asset to be well protected, the F-35 programme maintains a complex global supply chain of more than 1,500 sub-contractors across ten nations. With even the prime contractor Lockheed-Martin unable to fully track the level of security assurance delivered at each stage of the supply chain, there is a credible risk that Russian intelligence agencies might target a subcontractor. If successful, Russia could insert malware onto either the F-35 itself or a critical ground support system. Once achieved, malware might lay dormant and undetected until triggered during a conflict with the West[1268].

Adding depth to this issue, a declassified secret report from the US Inspector General's Office further notes that the F-35 includes potentially vulnerable Commercial Off the Shelf (COTS) technologies from a range of providers[1269]. When combined with the potential supply chain issues, such information adds credibility to the risk of Russia exploiting opportunities to compromise the underlying technologies of a 'software-based aircraft…[that is known to be] susceptible to hacking'[1270].

[1268] Lockheed-Martin, "The Global F-35 Enterprise ".
[1269] US, "Audit of the Dod's Management of the Cybersecurity Risks for Government Purchase of Commercial Off-the-Shelf Items", ed. Inspector General of the US Department of Defence (2019), 2.
[1270] S. Jost, interview by Staff Writter, March 2019.

In considering these potential areas of exploitation, a serious concern emerges. Specifically, if Russia were to use its cyber capabilities to compromise any one of the F-35s potential cyber vulnerabilities it could remove the platform from NATO's defence of the Baltics. If such an attack were synchronised with similar attacks on other air platforms and supporting infrastructure, Russia could disrupt the keystone capability of air power altogether. Though NATO could in time recover from such cyber attacks, recovery would not be instantaneous.

Therefore, if Russia actively learns from its failures in Ukraine to effectively deliver cyber planning and cross domain activity it may synchronise cyber attacks with nonlinear strategies including conventional attack to undermine NATO air power. If achieved, Russia could at speed overrun the vastly outnumbered AFP and militarily secure the Baltics in, as RAND predicts, little more than 60 hours[1271]. Though it is acknowledged that there are many complex steps to achieving this worst-case scenario, what the case study illustrates is that whilst difficult, the Russian cyber threat to not only Western air power but the West at large is credible.

Reflecting on this, a repeat of the conclusion on the Taiwanese case study is in part found. Specifically, Russia is potentially able to employ cyber means to target Western air power's cyber vulnerabilities. If successful, the strategic importance of the Western air deterrent could be lost or compromised, and Russia could with greater ease excerpt control over the Baltics. Through this, a credible cyber risk to Western air power which may undermine Western strategic advantage is found. Furthermore, as observed in the Taiwanese case study, the uncertainty of the cyber risk may even adjust the West's strategic calculus. However, because of the NATO Article 5 assurances as opposed to US strategic ambiguity in the Asia-Pacific, this is acknowledged as a potential but less prevalent consideration in the Baltics.

Taken collectively, this Baltic case is not as definitive, or as impactful in depth, as the Taiwanese example. Nonetheless, it still offers evidence to support the thesis'

[1271] Shlapak and Johnson, *Reinforcing Deterrence on Nato's Eastern Flank: Wargaming the Defense of the Baltics*, 1.

assertions on the dangers associated with air power's cyber risk. Notably, Western air power has been shown as a vital capability in deterring Russia and the cyber risk to it could, if realised, undermine Western strategic advantage.

Iran and the Strait of Hormuz

Having explored the potential cyber risk emerging from great power competition in the form of the PRC and Russia, this final case study will consider the risk from a regional power: Iran. To do so, it will focus on its potential disruption of the Strait of Hormuz.

Playing 'a strategic and psychological role in the world energy market', the Strait which separates Iran from the Western aligned Gulf states of Oman and the United Arab Emirates (UAE) creates a 30 mile wide gateway into the Persian Gulf[1272]. Though such proximity would itself be a touchpoint for instability, it is also the route through which one-third of the world's sea-trade in oil passes[1273]. Totalling on average 21 million barrels a day, its closure would immediately have impact causing oil prices to 'skyrocket'[1274].

This combination of Western-Iranian tensions and global importance has unsurprisingly made the Strait a source of tension ever since the 1979 Iranian Revolution[1275]. On a purely legal standing, the Strait is under the 1982 UN Convention on the Law of the Sea (UNCLOS) given protected status. Notably, Article 44 asserts that 'states bordering straits shall not hamper transit passage'[1276]. However, whilst Iran signed UNCLOS it did not ratify it. Instead, Iran passed its own national maritime law in 1993 which allows 'innocent passage'

[1272] For the quote, see:
F. Nadimi, "The Irgc and the Persian Gulf Region in a Period of Contested Deterrence", *The Middle East Institute,* (2021): 4.
For the geography of the Strait of Hormuz, see:
Robert Strauss Center, "Strait of Hormuz: Assessing the Threat to Oil Flows through the Strait", (University of Texas 2022).

[1273] A. Ma, "How the Strait of Hormuz, a Narrow Stretch of Water Where Ships Carry $1.2 Billion of Oil Every Day, Is at the Heart of Spiraling Tensions with Iran", *Business Insider* (2020).

[1274] C. Krauss, "Oil Price Would Skyrocket If Iran Closed the Strait of Hormu", *New York Times*, 4 January 2012.

[1275] Nadimi, "The Irgc and the Persian Gulf Region in a Period of Contested Deterrence", 4.

[1276] United Nations, "United Nations Convention on the Law of the Sea (Unclos)", (1982).

under certain conditions but does not recognise it under the legal definition of an 'international strait'.

In practice this means that Iran will allow foreign vessels to navigate through what it considers to be its territorial sea if they respect all Iranian regulations and are not perceived to pose a threat to Iran. However, if Iran deems there to be a threat it can under its interpretation of the law close the Strait[1277]. Challenging this position, and defending the principles of UNCLOS, Western states operating in cooperation with their regional allies have for decades sought to prevent Iranian control by asserting FoN[1278]. Given the maritime environment, this effort has focused on naval capabilities led principally by the USN Fifth Fleet supported by UK Royal Navy (RN) vessels operating out of Bahrain[1279]. Adding depth, the US and UK are also supported by a broader international coalition coordinated by the International Maritime Security Construct (IMSC)[1280].

Adding to this naval commitment, Western air power also plays a key role in delivering a multi-layered maritime security framework. Supporting the IMSC through airborne surveillance which 'keeps watch over the tight channels', the air power component ranges from small UAVs and helicopters operated from naval vessels to large UAVs, fast jets and supporting platforms operating from permanent regional air bases[1281].

Considering first the aerial surveillance support these assets provide, the West demonstrated even in the wake of Iran's hostile downing of a US UAV in 2019 that these operations were too important to pause. With General David Goldfein,

[1277] Ibid.
[1278] A. Daolio, "Arab Allies Must Step up to Defend Freedom of Navigation in the Gulf", (2019).
[1279] For the USN Fifth Fleet, see:
US, "Eisenhower Carrier Strike Group Enters 5th Fleet", ed. UN Naval Forces Central Command Public Affairs (2021).
For UK RN operations in the Strait of Hormuz, see:
UK, "Operation Kipion", ed. Royal Navy (2022).
A. MacAskill, Saul, J. , "Britain Begins Escorting All Uk Vessels through Hormuz Strait", *Reuters* 25 July 2019.
[1280] For broader international maritime support, see:
N. Childs, 27 August 2019, https://www.iiss.org/blogs/military-balance/2019/08/naval-capability-challenges.
For depth on the IMSC, see:
International Maritime Security Construct, "An International Approach", ed. IMSC (2022).
For further depth on naval cooperation in the Strait of Hormuz, including multi-national exercises, see:
L. Brooke-Holland, "Uk Forces in the Middle East Region", ed. House of Commons Library (2020).
F. Gardner, "First Joint Naval Exercise by Israel and Gulf States Signals Iran Worries", *BBC News*, 15 November 2021.
[1281] S. Snow, "This Is How the Us Military Is Protecting the Strait of Hormuz", *Military Times* 29 December 2019.

USAF Chief of Staff, asserting after the incident that 'we're continuing to fly, and we will continue to fly', a game of 'drone chicken' with Iranian air defences was created in which Western UAVs skirted Iranian airspace and Iran threatened to retaliate. Despite the high stakes of escalation, the Wests unwillingness to withdraw assets underlines both the importance of the Strait and the air power securing it[1282].

Though this surveillance effort remains keystone, the regional land-based airfields alongside US and potentially UK aircraft carriers allows the West to also deliver crewed strike capabilities when required. For example, responding to the Iranian linked hostile use of UAVs to attack commercial Motor Tanker (MT) Mercer Street in 2021, the US deployed an undisclosed number of F-22 Raptor fighters to the UAE [1283] . Further supported by routine US aircraft carrier deployments such as the USS Nimitz transiting through the Strait in 2020, the scope and depth of the West's regional air power strike capability has been demonstrated[1284].

Reflecting on this Western intent to deter Iran from seizing control of the Strait of Hormuz, and its considerable maritime and air power assets employed to achieve this, it is unsurprising that it has in balancing Iran's intent to become a regionally dominant military created a tinderbox. Exploring how in practice this might ignite, commentators point to catalysts including the Biden Administration's delays in repairing the damage inflicted by the Trump Administration, the Iranian 2021 election of the hard-line President Ebrahim Raisi, and a shortening timescale for Iran's achievement of a viable nuclear capability[1285]. Considering the potential end state of these issues and offering lenses through which to explore Iranian

[1282] For the quote, see:
D. Goldfein, interview by V. Insinna, 27 June 2019.
For depth on Iranian air defences, see:
S.J. Frantzman, "Iran Claims Its Air Defense Confronted Two Us Drones During Recent Drill", *Jerusalem Post*, 9 November 2021.

[1283] For the attack on MT Mercer Street, see:
F. Gardner, "Mercer Street: Tanker Blast Evidence Points to Iran, Says Us", *BBC News* 7 August 2021.
For the F-22 deployment, see:
Suciu. P., "U.S. Air Force Sends F-22s to the Uae after Surge in Houthi Attacks", *The National Interest,* (2022).

[1284] Staff Writer, "Us Carrier Transits Strait of Hormuz Amid Tensions with Iran", *AP*, 18 September 2020.

[1285] For background on increased tensions, see:
International Crisis Group, "10 Conflicts to Watch in 2022", (International Crisis Group, 2022).

cyber power, the Strauss Centre offers potential scenarios for conflict. Amongst these, the one in which Iran strikes first is perhaps the most convincing[1286].

Built on the premise that Iran has developed a respect for Western military capabilities following the US's decisive victory in Operation Praying Mantis, it hypothesises that when the tinderbox ignites Iran is likely to take the initiative and strike first[1287]. In this, the Strauss Centre argues that Iran would, in the right circumstance, conduct a methodical no-notice multi-layered attack in the Strait to achieve strategic advantage[1288]. Whilst such attack would, the scenario outlines, focus on mining the Strait followed by well-practiced attacks using anti-ship cruise missiles and small suicide boats, Iran will know that to be successful it must blunt the Western air delivered surveillance and strike capabilities.

Despite operating one of the largest air forces in the region with approximately 350 fighter aircraft, Iran's ability to achieve this via conventional means is hampered by an ageing and relatively unadvanced fleet[1289]. Even when backed by improved air defences and domestic advancements in UAV technology, Iran remains no match for the advanced air power of the West and its regional allies[1290]. Given this, a logical route for Iran to undermine Western air power, gain strategic advantage and achieve its intent in the Strait is through cyber.

[1286] For the Strauss Centre scenarios, see:

Robert Strauss Centre for International Security and Law, "Strait of Hormuz: Assessing the Threat to Oil Flows through the Strait", (University of Texas, 2022).

[1287] Operation Praying Mantis refers to the US's reaction to the Iranian mining of the Gulf in 1988 and the subsequent damaging of the USS Samuel B. Roberts. In response, the US attacked 2 Iranian oil platforms. When Iran attempted to retaliate, the US destroyed approximately a quarter of Iran's conventional naval fleet. Viewed in retrospect, Iran learned that to achieve regional impact against the US it must in any conflict immediately take the strategic imperative and gain the upper hand. For depth on Operation Praying Mantis, see:

K. Katzman, Nerurkar, N., "Iran's Threat to the Strait of Hormuz ", ed. Congressional Research Service (2012).

[1288] Specific events identified by the Strauss Centre include Iran responding to sanctions and the IRGC acting independently and then being backed by the state to avoid national embarrassment (as occurred in the kidnapping of UK RN and Royal Marine (RM) personnel in 2007). For depth, see:

Robert Strauss Centre, "Strait of Hormouz - Iran Strikes First ", (University of Texas 2022).

[1289] Iranian current air power is reported to range from the 1970s US made F-5, F-14 and F-4, through to the 1980s MIG-29's and the 1990s PRC made J-7. For details, see:

D. Axe, "Why Is Iran's Airforce So Outdated?", *The National Interest,* (2021).

[1290] For depth on Iranian air defence, see:

N. Carl, "The Growing Iranian Threat around the Strait of Hormuz", (Critical Threats 2020).

Staff Writer, "Inauguration of Persian Gulf Air Defense Command Center", *YJC* 7 October 2019.

For Iranian UAV advances, see:

M. Soliman, "Home Drones Are Re-Engineering the Geopolitics of the Middle East Drones Are Re-Engineering the Geopolitics of the Middle East", *Middle East Institute,* (2022).

Considering the cyber options available to Iran, one would expect it to bring to bear its full breadth of capabilities developed and demonstrated throughout the 21st century. Beginning with left-of-launch means, Iran has shown through attacks on Saudi Aramco and a New York dam that it is able to target and disrupt supporting infrastructure[1291]. It has also shown in its response to the Stuxnet attack that it can learn from the lessons of others[1292].

Reflecting on examples including the PRC's alleged attack on Mumbai's power network, it can be expected that Iran would employ cyber to target and disrupt the Western air bases in locations including Oman and Qatar[1293]. Likely to be achieved via a breadth of attack vectors ranging from targeting SCADA systems integral to fuel supplies or power to the accessing and wiping of data on supporting networks, it is possible that through such pre-emptive cyber means Iran could disrupt or even prevent Western air assets from operating. If conducted in a period when a US carrier group was not in the area, and timed to coordinate with other conventional attacks, Iran could gain a window of operational freedom in which it was only opposed in the air domain by maritime based helicopters and small UAVs. By levelling the playing field in this manner via cyber means for a short period, Iranian air power could despite its ageing nature be decisive in allowing strategic advantage to be achieved.

Considering a further viable left-of-launch attack vector, Iran could also use its proven intent and capability to target military personnel as it did in its exploitation of Facebook[1294]. If this capability were to be redirected against Western personnel serving in the Gulf, or personnel from the West's regional allies including Oman, Bahrain, Qatar and Saudi Arabia, there is a potential that cyber means could be used to subvert personnel leading them to act as malicious

[1291] For Saudi Armco attacks, see:
US, "Iran - Current Topics".
For the New York Dam attack, see:
Kennedy, "How Iran Would Wage Cyber War against the United States".

[1292] US, "Iran - Current Topics".

[1293] For detail on the PRC attack on Mumbai's power grid, see:
Staff-Writer, "Mumbai Power Outage in October May Have Been Result of 'Cyber Sabotage'".

[1294] For depth on the Iranian use of Facebook and other websites to target Western military personnel, see:
Gleicher, "Iranian Hackers Targeted Western Militaries".
Team, "Tortoiseshell Group Targets It Providers in Saudi Arabia in Probable Supply Chain Attacks".
Stoica, "Social Engineering as the New Deception Game", 61.

insiders and disrupt air power. Alluding to a digital underpinning to more traditional subversion and sabotage against air platforms and its supporting infrastructure, the scenario is supported by the known and growing hostile activities of the Iranian Ministry of Intelligence and Security (MOIS)[1295].

Whilst MOIS overseas activities have traditionally focused on the surveillance, abduction and killing of Iranian expatriates opposed to the ruling regime, its foreign powers were formally expanded in 2017. This change resulted in a growth of its overseas operations. With these reportedly including the active deterrence and harassment of its regional rivals through either targeting disaffected individuals or supporting proxy groups, a situation was established in which MOIS would be expected to support pre-planning for a conflict. With the above cyber means also tried and tested by Iran in the identification of targets for MOIS to pursue, a viable scenario is created in which Iran uses exploits such as the Facebook example to cultivate people who at a strategic time could sabotage air platforms or supporting infrastructure. In doing so, a further cyber enabled left-of-launch attack vector on air power is identified[1296].

Following this initial preparatory phase in which left-of-launch attacks blunt the air power of the West and its regional allies, Iran has also displayed an ability to use cyber to directly target Western air power. Though publicly reported examples are limited to its 2011 hijacking of a US Sentinel UAV, such a capability if repeated and combined with its growing air defence system could further disrupt a Western and allied response.

Taken collectively, this combination of pre-emptive left-of-launch and direct cyber attacks could viably affect both Western aerial surveillance and strike assets. Shown through the above narrative of Iran's worsening relationship with the West to indicate a credible intent, and via the discussion on Iran's cyber capabilities as

[1295] For a history of and background on MOIS, see:
C.A. Wege, "Iranian Counterintelligence", *International Journal of Intelligence and CounterIntelligence,* 32, no. 2 (2019): 273.

[1296] For depth on MOIS and Iranian overseas intelligence activities, see:
S. Golkar, "Iran's Intelligence Organizations and Transnational Suppression", *The Washington Institute for Near East Policy,* (2021).
A.M. Tabatabai, Martinin, J., Wasser, B., "The Iran Threat Network (Itn): Four Models of Iran's Nonstate Client Partnerships", (2021).

potentially achievable, one can conclude that the likelihood of the scenario emerging is credible. Given this and the assessment that though recoverable in a cyber sense such activity would for a period degrade the situational awareness of the West and its allies, the use of cyber to support conventional capabilities could create a strategically important first-strike window.

If successfully capitalised on through conventional capabilities, Iran may deny the Strait to commercial traffic and gain military control. Though such effects could be recovered from, and the West would be expected to reassert control over the Strait, the political impact of such an Iranian victory would be momentous. Likely to embolden Iran into further action, the events could, with cyber as an undercurrent of facilitation, strategically shift the situation in the Middle East.

Conclusion: Assessing the Cyber Risk to Western Air Power

Drawing together the previous discussions, this Chapter initially summarised how this thesis established the cyber risk to air power as a credible concern which could undermine a state's role or even lead to events with existential ramifications. To test this assertion, the purpose of the third Part of the thesis was identified as a representative case study of the West and aligned states. Using this sub-set of the international community as a vehicle, the Part would contextualise cyber vulnerabilities of and cyber threats to air power as a means of identifying globally relevant conclusions. In drawing this intent together, it was finally noted how this closing Chapter of Part 3 would test assertions derived from specific state focused discussions through three scenario-based case studies.

In the first case study, the potential of the PRC attempting to achieve reunification with Taiwan through force was examined. Through this, it was concluded that the cyber risk to Western air power was not simply proven but shown to have depth. Notably, on one level, it demonstrated how in a potential conflict the PRC could exploit direct and indirect cyber vulnerabilities within both Taiwanese and US air power to undermine Western strategic advantage. Adding depth it was further concluded that the mere potential impact of cyber risk manifesting may be enough to prevent US involvement in a crisis. In such circumstances, cyber risk to Western air power was identified as reaching a level of strategic importance equal to other capabilities such as the nuclear deterrent.

Next, considering a potential attack on the Baltics by Russia, similar but not such stark conclusions were reached. Specifically, Russia was concluded to have the potential to employ cyber means to target Western air power's cyber vulnerabilities. If successful, the strategically important Western air deterrent could be lost or compromised. Though it was also noted that this might extend to a deterrence, it was accepted that NATO Article 5 assurances as opposed to US strategic ambiguity in the Asia-Pacific make this less likely. On this basis, the cyber risk to Western air power was found to be credible and had the potential to impact Western strategic advantage. However, it was ultimately judged as unlikely to be as decisive a factor as in the Asia-Pacific.

In a final examination of Iran and a potential intent to control the Strait of Hormuz, it was found that Iran does not demonstrate as significant a cyber risk as the PRC or Russia. However, it was further asserted that when taken collectively the combination of Iranian pre-emptive left-of-launch and direct cyber attacks could affect both Western aerial surveillance and strike assets. Potentially offering a window of strategic advantage, this might allow Iran to deny the Strait to commercial traffic and gain military control for a short period. Whilst recoverable for the West, the political outcome of such events was highlighted as having potentially momentous impact in the Middle East. Based on this, it can be concluded that though not as significant for the West as the Taiwanese or Baltic examples, the ability of cyber risk to undermine Western air power and have wider strategic impact was again confirmed.

Taken as a whole, the three case studies have endorsed the findings of the previous chapters and further proven the thesis' assertions. Specifically, all have shown how air power as a vital capability plays a key role in assuring Western strategic advantage whether in the Asia-Pacific, Europe, or the Middle East. Further, though varying between regions and actors, all the case studies showed that the air power of Western or aligned states have cyber vulnerabilities and that these could be exploited by credible cyber threats.

Beyond this, the case studies further reinforced the assertion that the impact of air power's cyber risk is also relative, not absolute. Ultimately, the level of concern becomes inverse to the size and resource of the state, or for the Baltics the Alliance which it is a part of. Following this logic, it can be argued that larger states and Alliances are more resilient than their smaller counterparts.

Taken in their totality and reflected against the vulnerability and threat discussions of the preceding chapters, the case studies have reinforced the overarching conclusions. Notably, whilst the overall impact may vary, what remains constant is that cyber risk has the potential to cause the loss or compromise of Western and aligned air power. This, if realised, could undermine Western strategic advantage and may in turn threaten the continuance of a role or, in extremis, have existential impact for smaller states.

Part 4: Conclusions, Observations and Recommendations

Conclusions, Observations and Recommendations

This thesis has argued that though created through operational causes, air power's cyber risk has strategic consequences. Employing an extensive body of existing academic, governmental, industry and media literature at the operational and strategic levels to build the argument, the thesis challenges current thinking by identifying a distinct gap in knowledge. Specifically, academia has not to date charted the causal relationship between the operational and strategic levels of air power's cyber risk. This gap, because of an associated lack of understanding and management, has created a risk that the maturing operational causes will act as a catalyst to the identified strategic consequences.

To address this gap, the thesis adopted a risk management methodology that meticulously developed the argument from the causes of the risk through to its consequences. However, before this risk approach could begin, it was first necessary in the foundational discussions of Part 1 to identify the gap in knowledge through a literature review in Chapter 1 before introducing the baseline concepts of cyber and IR in Chapters 2 and 3.

In offering this baseline, it was observed how a pragmatic approach must be adopted if academic research is to understand and address the real-world problem of air power's cyber risk. This was encapsulated in the holistic definition of cyber offered in Chapter 2 and the breaking down of the pedagogic walls by adopting a pluralistic paradigm offered in Chapter 3. In embracing these approaches, the thesis argued that for academics to successfully research real-world problems they must not be restricted by narrow definitional approaches. Based on this, it can be recommended that within the scope of researching air power's cyber risk, IR scholars must adopt a realist-constructivist paradigm and consider cyber to incorporate not only digital systems and networks but the physical infrastructure and people through which air power is delivered.

Turning next to the risk-based approach which guided the methodology through Parts 2 and 3, a series of operational and strategic level observations are offered.

Initially through an examination of the ‘first cause’ of state procurement of and reliance on air power in Chapter 4, it was confirmed how the literature across the forms of power and the translation of power to influence identify air power as an essential capability. Though this reliance on air power is shown to be relative and limited to states with the economic capability and whose role is tethered to global aspirations or who face an existential threat, a clear observation emerges. Specifically, those responsible for developing state strategy and meeting national aspirations must recognise how the ubiquity of air power allows it to deliver effect and meet objectives in numerous areas. Based on this observation, practitioners engaged in statecraft are recommended to not only prioritise air power to reach the true potential of a state but also recognise the wider cyber risk such decisions incur.

In the following examination of operational level cyber vulnerabilities at Chapter 5, the discussion ranged across the people, information, and real layers of cyberspace. Through this it was observed that due to previous failures to adopt a holistic approach to cyber, the operational level understanding of some areas remains less mature. It is therefore recommended that whilst practitioners must consider all elements of the holistic approach to cyber, researchers would be advised to focus on two areas of concern that remain poorly understood: the air power supply chain and the critical infrastructure relied on for air operations. Once understanding of these is matured through further focused academic study which must identify how they influence the strategic level consequences of the cyber risk, results must be reflected on and any relevant recommendations enacted.

In the final causal exploration of the operational level cyber threats to air power in Chapter 6, it was recognised that whilst cyber vulnerabilities are significant, they are not of concern unless targeted and exploited by cyber threats. Considering the ultimate argument that though emergent it is a matter of ‘when’, not ‘if’ cyber threats will reach a level of potency able to credibly disrupt air power, the necessity of a holistic approach to cyber is revisited. Notably, it is observed that some areas of cyber threats remain less understood and more likely to have impact than others. Citing left-of-launch attacks as a prominent example, there is a requirement for further academic research if practitioners are to be given the tools to counter the threat. Within this the research has also shown the supply chain to be the most concerning in terms of its breadth and potential impact on the viability of air power. It is therefore recommended that further research must be focused on the left-of-launch supply chain cyber threat to air power.

Concurrent to this, it was also observed through the literature that successful cyber attacks are routinely the result of ill-preparedness of defenders rather than the overwhelming offensive capability of attackers. It is therefore recommended that both air power practitioners and academics alike remain mindful of the need to translate the understanding of cyber threats into viable cyber defence. If this is not heeded, and recommended research into supply chain threats is not conducted, air power’s cyber risk will not only materialise but it will undermine air power’s viability and threaten the role of states or, in extremis, their survival.

Reflecting on the observations and recommendations offered through a review of Part 2 of the thesis, a common theme is identified: cyber vulnerabilities and threats to air power may represent operational causes, but in their manifestation they have strategic consequences by removing the capability states rely on to maintain role and survival. In understanding this causal link, it becomes necessary to enact the above recommendations so that the emergence of the causes can be managed and their impact through strategic consequences can be mitigated.

Having explored the three causes of air power’s cyber risk in Part 2, Part 3 employed a pragmatically narrowed case study focusing on Western and aligned states to explore the consequences. In delivery, this was broken down into three discussions: cyber vulnerabilities, cyber threats, and the collective risk.

Beginning in Chapter 7 with cyber vulnerabilities, three representative Western and aligned case studies of the US as a superpower, the UK as a residual great power and Taiwan as a Western aligned regional power were discussed. Viewed collectively, these case studies observed that all Western and aligned air forces are susceptible to cyber vulnerabilities that could undermine or remove their air power capabilities. Offering supporting evidence to the causal importance of cyber vulnerabilities discussed in Chapter 5, a recommendation can be offered on the importance of practitioners to adopt a far-reaching approach to cyber security if Western and aligned air power is to remain viable.

It was further observed that the concern cyber vulnerabilities create is inverse to the size of the state. For example, although exposed to cyber vulnerabilities, as a superpower the US can mitigate these through breadth and depth. As such, it may be challenged but is not in danger of losing its role. In contrast, the UK as a residual great power may through cyber vulnerabilities see the loss or compromise of its relatively limited air power lead to an undermining of its 'Global Britain' role. Finally, for Taiwan the issue is raised to one of existential survival with cyber vulnerabilities potentially removing a key element of national defence. It is therefore observed that though all states must mitigate air power cyber vulnerabilities, the issue is far more pressing for smaller states. These states are therefore recommended to invest heavily in mitigations if their keystone air capabilities are to be maintained and their role or even survival assured.

Shifting to consider cyber threats to Western and aligned air power, Chapter 8 explored representative examples of the PRC as a superpower in waiting, Russia as a great power pushing to maintain global relevancy and Iran as a regional power seeking to assure operational influence. In reviewing these case studies, it was observed that the cyber threats were cohesive in that all hold the credible ability to disrupt Western and aligned air power. Going further, however, it was also noted how the threats are distinct. Firstly, the PRC cyber threat is long-term, intent on gaining strategic advantage and deterring Western air power. Secondly, the Russian cyber threat is far more immediate and tied to conventional means to achieve strategic intent. Thirdly, the Iranian cyber threat may represent a less direct concern but remains one that could target air power and unbalance the region.

Given this complexity it was observed that there is no ‘one size fits all’ form of cyber with each threat distinct and likely to come to fruition at different times. To address this, academics and practitioners alike are recommended to approach cyber threats in a nuanced manner which appreciates a depth of understanding. By doing so, and by paying particular attention to the long-term monitoring of hostile states intent and capability, emergent cyber threats will be tracked, developing cyber risk understood and the need to focus cyber defences defined. If achieved, operational building blocks will be solidified and the strategic implications on states roles and survival controlled.

Leading the case study to its final discussion, and seeking to test the conclusions already drawn, Chapter 9 brought together vulnerabilities and threats through three potential scenarios: an attack on Taiwan by the PRC, an attack on the Baltics by Russia and an attempt to exert control over the Strait of Hormuz by Iran. Considered together, the case studies endorsed previous observations. Notably, all the scenarios demonstrated how air power is a vital capability for Western and aligned states as they seek to maintain their roles and assure their survival. The scenarios further demonstrated that the air power relied on to achieve these aims holds both exploitable cyber vulnerabilities and are faced by credible cyber threats. To manage these and ensure operational concerns do not snowball into strategic implications, the West and its allies are urged to recognise the observations raised in this thesis and enact the recommendations.

Reflecting on the collective conclusions, observations and recommendations presented above, it is evident that the maturity of the cyber risk to air power can be questioned. However, operational level causes are already significant, their causal relationship with the strategic level confirmed and, when the associated cyber risk is realised, the potential to achieve significant consequences demonstrated. When coupled with the ever-evolving nature of the digital domain, air power’s cyber risk becomes a matter of ‘when’, not ‘if’, it will emerge as a route through which roles and even national survival will be threatened.

Though an assertion reinforced for a predominance of Western and aligned states through the case study presented in Part 3, this reality has a global truth. Specifically, for the predominance of states who rely on air power, operational causes of the cyber risk will lead to the emergence of credible strategic consequences. Further, with the existing gap in knowledge on the operational to strategic causal relationship preventing effective mitigations, it is observed as highly likely that air power's cyber risk could redefine the geopolitical landscape of the 21st century.

This assertion is, however, caveated by an acknowledgment that the cyber risk to air power is not absolute, but relative. Firstly, only states seeking a global role or those facing an existential threat are likely to become reliant on air power. Secondly, of those dependent on air power, larger states may not be able to prevent the causes manifesting, but their breadth and depth of capability are likely to insulate them from the most severe consequences. Therefore, air power's cyber risk becomes situationally specific and inverse to the size of the state.

It is further noted that though these assertions offer significant concern, especially for regional and great states which have less resources but are still reliant on digitally enabled air power, the conclusion is not unique. Rather, it is representative of the challenges that are perpetually reflected in emergent technologies. An assertion explored by Gladwell in his book *The Bomber Mafia,* he argues that with the advent of new ideas or innovations it can be 'obvious to all that they will upend our world'[1297]. Though written in the context of Second World War strategic bombing, his sentiment resonates with the digitisation of air power.

Continuing his argument by asserting that 'when some new, shiny idea drops from the heavens, it does not land softly in our laps…[but] lands hard and shatters', Gladwell could easily be referring to cyber risk. Specifically, the 'shiny new idea' of digitisation has 'dropped from the heavens' and has enhanced air power as strategic bombing did in the Second World War. However, as with the

[1297] M. Gladwell, *The Bomber Mafia* (London: Penguin Books, 2021), 8.

challenges for strategic bombing which caused a 44 percent death rate in the RAF Bomber Command by 1943, contemporary vulnerabilities and threats may also cause digitally enhanced air power to 'land hard and shatter'[1298].

When considered against early air power thinking, the logic of adversaries pursuing this cyber risk to air power becomes starker. Taking Douhet's 1921 book *The Command of the Air* as an example, he asserted that to counter the critical capability of air power 'it is easier and more effective to destroy the enemy's aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air'[1299]. Though arguing at the time for the value of strategic bombing, when translated to this age of digital enablement Douhet's assertions add emphasis to cyber risk with cyber means becoming increasingly capable of destroying the 'nest and eggs' of air power before flight is achieved. Leading to the state level strategic impacts on role and survival discussed above, cyber risk becomes of grave concern to not only air power academics and practitioners but those engaged in statecraft.

Whilst true, it is also the case that any risk can be managed. As the risk of strategic bombing was mitigated in the 20th century by advancements in fighters providing escorts to vulnerable bombers, cyber risk can be mitigated by the effective training of people, the development of robust processes and the delivery of secure technologies. However, to be effective, those developing and delivering such measures must achieve strategic effect by reflecting on lessons learnt and, through in-depth research, bridge gaps in knowledge on the relationship between operational causes and strategic consequences.

Responding to this reality, the thesis has, in conclusion, employed a risk management framework to demonstrate that the cyber risk to air power though operational in its causes is strategic in its consequences. In doing so, it goes beyond the current literature which remains bracketed in either operational discussions of technical risk or scholarly considerations of strategic impact.

[1298] G.D. Davis, *Bombing the Axis Powers* (Alabama: Air University Press, 2006), 25.
[1299] Douhet, *The Command of the Air*, 49.

Identifying a distinct gap in knowledge, an imperative emerges for academics and practitioners to explore the relationship between operational causes and strategic consequences.

If achieved using the observations and recommendations presented in this thesis as a handrail for further research, a catalyst will have been offered that will nurture the growth of knowledge, prevent operational challenges creating strategic consequences and, ultimately, protect the roles and even survival of states. If this is achieved, air power’s vital 'nest and eggs' will be shielded from harm and the repercussions of a 'hard landing' avoided.

However, any failure to bridge the gap in knowledge will likely allow an uncertain reality to manifest in which air power's cyber risk casts a dark shadow, erodes roles, endangers state survival, and reshapes the geopolitical landscape. The power to choose which future manifests is in our hands: this thesis has laid the groundwork, but it is the academic and practitioner community who must seize the moment, act in synergy, and confront the operational causes to prevent the strategic consequences. If successful, air power’s cyber risk could be mitigated to a point at which its most destructive impacts are consigned to the annals of history, rather than materialising as a formidable and decisive factor of the 21st century.

Bibliography

Achen, C. H., and D. Snidal. "Rational Deterrence Theory and Comparative Case Studies". *World Politics* 41, no. 2 (1989): 143-69.

Acheson, D. "Dean Acheson's Speech to the National Press Club " news release, 1950, https://web.viu.ca/davies/H102/Acheson.speech1950.htm.

Ackerman, E. . "U.S. Army Considers Replacing Thousands of Soldiers with Robots". *IEEE Spectrum* (22 January 2014).

Adams, A., and M.A Sasse. "Users Are Not the Enemy". *Communications of the ACM* 42, no. 12 (2010): 40-46.

Adams, C. . "Sdr Takes Flight". *Aviation Today* (1 February 2013).

Adams, J. *Risk* London: Routledge Taylor and Francis Group, 1994.

Adamsky, D. . "Cross-Domain Coercion: The Current Russian Art of Strategy". *Proliferation Papers* 54 (2015).

Addison, P. "The Impact of the Second World War." In *A Companion to Contemporary Britain: 1939-2000*, edited by P. and Jones Addison, H. , 3-18. Oxford: Oxford University Press, 2005.

Adgie, K.P. "Applying Clausewitz to 21st Century Landpower Theory": US Army War College 2010.

Adler E. "Complex Deterrence in the Asymmetric-Warfare Era." In *Complex Deterrence* edited by T.V. Paul, 85-130. Chicago: University of Chicago Press, 2009.

Adler, E. , and M. Barnett. *Security Communities* Cambridge1998.

Agency, Defense Security and Cooperation. "Japan - F-35 Joint Strike Fighter Aircraft ", 2020.

Agrawal, H., J. Alberi, L. Bahler, J. Micallef, and A. Virodov. "Detecting Hidden Logic Bombs in Critical Infrastructure Software". *International Conference on Information Warfare and Security* 1 (2012).

Ahrensdorf, P. J. . "Thucydides' Realistic Critique of Realism". *Polity* 2, no. Winter (1997): 231-65.

Ajilli, H., Rouhi, M. . "Iran's Military Strategy ". *Survival* 61, no. 6 (2019): 139-52.

Akbar, M.S. "Obama or Romney: What It Means for a Pakistani Living under Drones", *CNN Political Op-Ed*, 6 November 2012.

Al Rodhan, N. "Strategic Culture and Pragmatic National Interest". *Global Policy* (22 July 2015).

Alderton, M. . "Airborne Isr", *Trajectory Magazine*, 4 December 2013.

Alexander, H. . "Who Is Chelsea Manning?", *The Telegraph*, 2017.

Allen, M.A., E. Flynn Michael, M. Machain C, and A. Stravers. "Outside the Wire: Us Military Deployments and Public Opinion in Host States". *American Political Science Review* 114, no. 2 (2020): 326–41.

Allison, G. "Do British Fighter Jets 'Protect' Irish Airspace?". *UK Defence Journal* (19 June 2022).

———. "F-35b Enters Operational Service". *UK Defence Journal*, no. 3 August (2015).

———. "Raf to Introduce Additional Swarming Drone Squadron". *UK Defence Journal* (14 July 2021).

———. "The Thucydides Trap: Are the Us and China Headed for War?", *The Atlantic*, 24 September 2015.

———. "Typhoon Life to Be Extended Two More Squadrons to Be Created". *UK Defence Journal* (23 November 2015).

———. "What Is the Purpose of Tempest". *UK Defence Journal* (1 September 2018).

Allison, G. . "What’s So Good About the F-35 Anyway?". *UK Defence Journal* (23 February 2019).

Anderson, J. P. "Computer Security Threat Monitoring and Surveillance ". In *User Profiling in Intrusion Detection: A Review*, edited by J. Peng, K. Choo and H. Ashman, 14-27. Journal of Network and Computer Applications, 2016.

Andrade, T. *How Taiwan Became Chinese: Dutch, Spanish, and Han Colonization in the Seventeenth Century.* New York: Columbia Unveristy Press, 2010.

———. "The Rise and Fall of Dutch Taiwan, 1624–1662: Cooperative Colonization and the Statist Model of European Expansion". *Journal of World History* 17, no. 4 (2006): 429-50.

Annan, K.A. "We the Peoples: The Role of the United Nations in the 21st Century ". New York: United Nations, 2000.

Annan, K.A. . "Secretary-General’s Annual Report to the Un General Assembly ", edited by UN General Assembly. New York United Nations 2005.

Ansip, A. . "Estonian Pm Insists That Cyber Attacks Came from Kremlin Computers", *The Baltic Times*, , 6 August 2007.

Applebaum, J. . "Nsa Preps America for Future Battle", *Das Spiegel*, 2015.

Aquilino, J. "China Threat to Invade Taiwan Is 'Closer Than Most Think', Says Us Admira." By Staff Writer. *The Guardian* (23 March 2021).

Armitage, M., and R. A. Mason. *Air Power in the Nuclear Age: 1945-84* London: MacMillan), 1985.

Arquilla, J., and D. Ronfeldt. *Swarming and the Future of Military Conflict.* Santa Monica: RAND, 2000.

Arquilla, J., and D. Ronfeldt. "Cyberwar Is Coming!". *Comparative Strategy* 12, no. 2 (1993): 141–65.

ArsTechnica. "Open Forum Message Board", 2009.

Arthur, C. . "Skygrabber: The $26 Software Used by Insurgents to Hack into Us Drones", *The Guardian*, 17 December 2009.

Ashworth, L.M. . "Where Are the Idealists in Interwar International Relations?". *Review of International Studies* 32 (2006): 291-308.

Aspin, L. "Report on the Bottom-up Review", edited by Department of Defence, 1993.

Atkinson, C. *Military Soft Power: Public Diplomacy through Military Educational Exchanges.* Lanham: Rowman & Littlefield, 2014.

Augustine. *The City of Gods: Against the Pagans* Cambridge: Cambridge University Press, 413-426 BC.

Aung, Y. "Operation Shadowhammer", edited by SecureList: Kaspersky 2019.

Austin, L.J. "Senate Armed Services Committee Advance Policy Questions for Lloyd J. Austin Nominee for Appointment to Be Secretary of Defense", edited by US Senate, 2021.

Australia. "Strong and Secure: A Strategy for Australia’s National Security", edited by Department of the Prime Minister and Cabinet. Australia Australia 2013.

Axe, D. "Taiwan Might Experience Buyers Remorse over the F-16 Fighter". *The National Interest* (29 January 2022).

———. "Why Is Iran's Airforce So Outdated?". *The National Interest* (6 August 2021).

Bachmann, S., Dowse, A., Gunneriusson, H. "Competition Short of War–How Russia's Hybrid and Grey-Zone Warfare Are a Blueprint for China's Global Power Ambitions". *Australian Journal of Defence and Strategic Studies* 1, no. 1 (2019).

Bader, J.A. "The U.S. And China's Nine-Dash Line: Ending the Ambiguity". *Brooking Institute* (6 February 2014).

BAE. "Cybersecurity Products: Data Diode " BAE Systems, https://www.baesystems.com/en/product/data-diode-solution.

Băhnăreanu, C. "The Evolution of Warfare from Classic to Hybrid Actions". *Strategic Impact* 2 (2015): 57-66.

Bailey, J. "Airlines Need to Embrace It System Modernization: Here's Why". *Simple Flying* (1 Dcember 2021).

Baizacq, T. *Understanding Securitisation Theory* London: Routledge, 2011.

Baker, B. "Us Navy's Triton Uas – Poseidon's Perfect Partner", *Naval Technology*, 9 November 2014.

Baker, P. . "Trump and Johnson, Together on the World Stage, Eye Troubles Back Home", *The New York Times*, 24 September 2019.

Baker, S. . "The Boeing 737 Max Crashes Have Revived Decades Old Fear About What Happens When Airplane Computers Become More Powerful Than Pilots", *Business Insider*, 17 February 2020.

Baldor, L.C. "Flashy Drone Strikes Raise Status of Remote Pilots", *Boston Globe*, 12 August 2012.

Ball, J. . "How Chinese Expansionism Fuels an Expansionist Foreign Policy", *Global Security Review*, 10 June 2019.

Bank, World. "Military Expenditure (% of Gpd) – United Kingdom ", 2019.

Banka, A. "The Breakaways: A Retrospective on the Baltic Road to Nato". *War on the Rocks* (4 October 2019).

Banner, S. . *Who Owns the Sky? The Struggle to Control Airspace from the Wright Brothers On* Cambridge MA: Harvard University Press, 2008.

Barkin, S.J. *Realist Constructivism* Cambridge Cambridge University Press, 2012.

———. "Realist Constructivism". *International Studies Review* 5, no. 3 (2003): 325-42.

———. *Realist Constructivism: Rethinking International Relations Theory.* Cambridge: Cambridge University Press, 2010.

Barns, J.E. "Us Says Iran Hacked Navy Computers", *The Wall Street Journal* 27 September 2012

Bassham, L.E., and T.W. Polk. "Threat Assessment of Malicious Code and External Attacks": National Institute of Science and Technology (NIST), 1992.

Bauer, B., and A.S. Patrick. "A Human Factors Extension to the Seven Layer Osi Reference Model". *Nortel Networks Research* (6 January).

Baylis, J., S. Smith, and P. Owens. *The Globalisation of World Politics.* Vol. 8, Oxford: Oxford University Press 2020.

BBC. "1991: Iraqi Scud Missiles Hit Israel - on This Day: 18 January 1991", *BBC News Online*, 18 January 2020.

———. "Armenia-Azerbaijan: Why Did Nagorno-Karabakh Spark a Conflict?", *BBC News Online*, 12 November 2020.

———. "Ex-Us Air Force Officer Monica Witt Charged with Spying for Iran", *BBC News Online*, 13 February 2019.

———. "Hiroshima Bomb: Japan Marks 75 Years since Nuclear Attack", 2020.

———. "Red Arrows Touch Down in China on World Tour." https://www.bbc.co.uk/news/uk-england-lincolnshire-37739750.

———. "The Rise and Fall of the Islamic State Group: The Long and Short Story." https://www.bbc.co.uk/news/world-middle-east-47210891.

———. "Solarwinds: Hacked Firm Issues Urgent Security Fix", *BBC News* 2020.

———. "Syria Fires on Israeli Warplanes", *BBC News Channel*, 6 September 2007.

———. "Us Cyber-Attack: Us Energy Department Confirms It Was Hit by Sunburst Attack", *BBC News Online*, 18 December 2020.

———. "Who, What, Why: How Can an Airport Run out of Fuel?", *BBC News Online*, 7 June 2012.

Beale, J. "Hms Queen Elizabeth: Why Is a Uk Aircraft Carrier Going on a World Tour?", *BBC News* 21 May 2021.

Bellwood, P, Dixon.E. "Austronesian Cultural Origins: Out of Taiwan, Via the Batanes Islands, and Onwards to Western Polynesia." In *Past Human Migrations in East Asia*, 23-39. New York: Routledge, 2008.

Beloff, M. "The Special Relationship: An Anglo-American Myth?: Essays for A.J.P. Taylor." In *A Century of Conflict: 1850-1950*, edited by M. Gilbert, 151-71. London: Hamish Hamilton, 1966.

Bender, J. . "The New F-35 Fighter Jet Can Be Taken Down without a Bullet Ever Being Fired", *Business Insider*, 18 February 2014.

Benitez, M. "F-15ex: The Strategic Blind Spot in the Air Force's Fighter Debate ". *War on the Rocks* (3 June 2019).

Bennett, C. "Fears Grow of Iran Cyber Attack". *The Hill* (22 November 2014).

Bennett, J. "China's New Y-20 Is the Largest Military Aircraft Currently in Production". *Popular Mechanics* (20 June 2016).

Berenskoetter, F., and M. J. Williams. "Thinking About Power." In *Power in World Politics* edited by F. Berenskoetter, 11-32. London: Routledge, 2007.

Bergmane, U. . "'Fading Russian Influence in the Baltic States". *Orbis* 64, no. 3 (2020): 479-88.

Berti, B. "Violent and Criminal Non-State Actors." In *The Oxford Handbook of Governance and Limited Statehood* edited by A. Draude, 273-94. Oxford: Oxford University Press, 2018.

Bertrand, N. "Iran Is Building a Non-Nuclear Threat Faster Than Experts 'Would Have Ever Imagined'". *Insider* (27 March 2015).

Betts, R.K. "Is Strategy an Illusion?". *International Security* 25, no. 2 (2000): 5-50.

Betz, D.J., and T. Stevens. *Cyberspace and the States: Toward a Strategy for Cyber-Power.* Abingdon: Routledge, 2011.

Bhutam N., Beck, S., Geib, R., Liu, H., Claud, K. . *Autonomous Weapon Systems: Law, Ethics and Policy* Cambridge Cambridge Universitry Press, 2016.

Biddle, B.J. "Recent Developments in Role Theory". *Annual Review of Sociology*, no. 12 (1986): 67-92.

Biden, J. "Taiwan Reports 'Large Incursion' by Chinese Warplanes for Second Day." By BBS News (25 January 2021).

———. "U.S. Concerned by 'Coercive' Chinese Actions in Taiwan Strait, Biden Tells Summit." *Reuters* (27 October 2021).

Biesecker, C. . "Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, Dhs Says", *Aviation Today*, 8 November 2017.

Birgbauer, P. "The Us Pivot to Asia Was Dead on Arrival ". *The Diplomat* (31 March 2022).

Blagden, D. "Two Visions of Greatness: Roleplay and Realpolitik in Uk Strategic Posture". *Foreign Policy Analysis* 15 (2019): 470-91.

Blair, A., Curtis, S. . *International Politics: An Introductory Guide* Edinburgh Edinburgh University Press, 2009.

Blair, T. "Don't Make the Mistake of Dismissing Iran's Ideology ", *Washington Posr* 8 February 2019.

Blakemore, E. . "How the East India Company Became the World’s Most Powerful Business", *National Geographic* 2020.

Blanchard, B. "U.S. Carriers in South China Sea, Taiwan Reports Further Chinese Incursion", *Reuters* 24 January 2022.

Blanchard, B., and Y. Lee. "Chinese Fighter Jets Enter Taiwan Airspace in ‘Threat to Regional Peace", *Independent*, 9 September 2020.

Bloxham, A. . "History of Recent Data Blunders by Government", *The Telegraph*, 14 October 2011.

Boeing. "F-15ex: More Capabiity. More Capacity. More Savings. ", 2022.

Bora, G., S. Bora, S. Singh, and M. Arsalan. "Osi Reference Model: An Overview". *International Journal of Computer Trends and Technology (IJCTT)* 7, no. 4 (2014): 214-18.

Borg, S. . "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework". *The Internet Alliance* (2010).

Bosco, D.L. *Five to Rule Them All: The Un Security Council and the Making of the World.* Oxford: Oxfrod University Press 2009.

Boutros, D.A. "Operational Protection from Unmanned Aerial Systems ". *Joint Military Operations, Naval War College* (15 May 2015).

Boynes, J. . "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations", edited by National Institute of Stnadards and Technology (NIST), 2021.

Boyson, S. . "Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical It Systems". *Technovation* 34 (2014): 342–53.

Brandom, R. . "Solarwinds Hides List of High-Profile Customers after Devastating Hack". *The Verge* (15 December 2020).

Brands, H. "The Eurasian Nightmare: Chinese-Russian Convergence and the Future of American Order". *Foreign Affairs* (22 February 2022).

Brenner, J. . "Interview with the Us House of Representatives Committee on Oversight and Government Reform." By J. Chaffetz. *Committee on Oversight and Government Reform* (2016).

Breslin, S. , and H.E.S. Nesadurai. "Who Governs and How? Non-State Actors and

Transnational Governance in Southeast Asia". *Journal of Contemporary Asia* 48, no. 2 (2018): 187-203.

Bridle, J. . "Rise of the Machines: Has Technology Evolved Beyond Our Control?", *The Guardian*, 15 June 2018.

Briefing, The Economist. "Aukus Reshapes the Strategic Landscape of the Indo-Pacific", *The Economist* 25 September 2021.

Brinkley, D. "Democratic Enlargement: The Clinton Doctrine". *Foreign Policy* 106 (1997): 110-27.

Brissett, W. . "Alis 2.02 Ready to Go", *Air Force Magazine*, 28 March 2017.

Broder, J. M., and D. Jehl. "Iraqi Army: World's 5th Largest but Full of Vital Weaknesses", *Los Angeles Times*, 13 August 1990.

Bronk, J. "Combat Air Choices for the Uk Government". *RUSI* (July 2020).

———. "Enter the Tempest". *RUSI Defence Systems* (16 ~July 2018).

Bronk, J. . "New British Plan Looks to Boost F-35 Numbers, but Is It Still Aiming for 138?" By A. Mehta. *Defence News* (23 March 2021).

Bronk, J., N. Reynolds, and J. Watling. "The Russian Air War and Ukrainian Requirements for Air Defence": RUSI, 2022.

Brook, C. . "Bad Rabbit Ransomware Hits Russia, Ukraine". *Digital Guardian* (7 August 2020).

Brooke-Holland, L. "The Combat Air Strategy: From Typhoon to 'Tempest'?", edited by House of Commons Library, 2018.

———. "Uk Forces in the Middle East Region", edited by House of Commons Library, 2020.

Brown, C.D. "China's Great Leap Forward". *Asian Studies* 17, no. 3 (2012): 30-34.

Brown, C.Q. "Accelerate Change or Lose ": United States Air Force 2020.

———. "The U.S. Air Force Just Admitted the F-35 Stealth Fighter Has Failed." By D. Axe. *Forbes* (23 February 2021).

Bull, H. *The Anarchical Society: A Study of Order in World Politics* London: MacMillan Press, 1977.

———. "Hobbes and the International Anarchy". *Social Research* (1981): 717-38.

Bunker, G. . "Targeting Cyber Attacks: How to Mitigate the Increasing Risk'". *Network Security*, no. 1 (2020): 17-19.

Burchill, S., A. Linklater, R. Devetak, J. Donnelly, M. Paterson, C. Reus-Smit, and J. True. *Theories of International Relations.* 3 ed. Basingstoke: Palgrave Macmillan, 2005.

Bush, G.W. "President's Radio Address: President Discusses the Beginning of Operational Iraqi Freedom", edited by The White House Archives, 2003.

———. "The President's State of the Union Address", edited by The White House Archives, 2002.

Bush, R. "The United States Security Partnership with Taiwan"". *The Brookings Institute* (November 2016).

Butt, A.I. "Why Did the United States Invade Iraq in 2003?". *Security Studies,* 28, no. 2 (2019): 250-85.

Buzan, B. "The English School: An Underexploited Resource in Ir". *Review of International Studies* 27, no. 3 (2001): 471-88.

Buzan, B. . *People, States and Fear* Brighton: Wheatsheaf Books, 1983.

Buzan, B., O. Wæver, and J. de Wilde. *Security: A New Framework for Analysis* London: Lynne Reinner Publishers, 1998.

Buzan, B., Wæver, O. *Regions and Powers: The Structure of International Security* Cambridge: Cambridge University Press 2003.

Byman, D. . "After the Storm: Us Policy toward Iraq since 1991". *Political Science Quarterl* 115, no. 4 (2001): 493-516.

Byman, D. L., M. C. Waxman, and J. Shapiro. "The Future of Us Coercive Airpower." In *Strategic Appraisal: United States Air and Space Power in the 21st Century* edited by Z. Khalilzad and J. Shapiro, 51-8. RAND: Santa Monica, 2002.

Cable, J. *The Geneva Conference of 1954 on Indochina.* New York: St. Martin's Press, 1986.

Cable, V. . "The Diminished Nation-State: A Study in the Loss of Economic Power". *Daedalus* 124, no. 2 (1995): 23-53.

Calvocoressi, P. *World Politics since 1945.* London: Longman 1996.

Cameron, D. "Uk Aid: Changing Lives, Delivering Results", edited by Department for International Development (DFID), 2011.

Cameron, D. and Blair, T. . "Cutting Aid Budget Would Hit Uk Influence, Two Former Pms Say", *Reuters Online*, 21 November 2020.

Cameron, L. "Lindy Cameron Speaking at the Rusi Annual Security Conference". *NSCSC Speeches* (14 June 2021).

Carberry, S.D. "Air Force Scrambles to Harden Weapons Systems", *FCW*, 21 September 2016.

Carl, N. "The Growing Iranian Threat around the Strait of Hormuz": Critical Threats 2020.

Carmont, D., Belo, D. . "War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare". *Canadian Global Affair Journal* (October 2018).

Carr, E.H. *Twenty Years Crisis: 1919-1939.* London: Palgrave Macmillan, 1939.

Carrol, W. . "A Closer Look at Israel's Syria Raid". *Defense Technology* (8 October 2017).

Carter, J. "Carter Lauds Shah of Iran, Dec. 31, 1977." By A. Glass. *Politico* (30 December 2018 1977).

Carter, N. "Russia Is Biggest Threat to Uk since Cold War, Say Head of British Army." By E. MacAskill. *The Guardian* (22 January 2018).

Casalicchio, E. and Toosi, N. . "Joe Biden Keeps Boris Johnson Guessing", *Politico* 21 September 2021.

Case, D.U. . "Analysis of the Cyber-Attack on the Ukrainian Power Grid". *Electricity Information Sharing and Analysis Centre (E-ISAC)*, no. March (2018).

Catrantzos, N. . "No Dark Corners: Defending against Insider Threats to Critical Infrastructure." 2009.

Cebrowski, A.K., and J.J Garstka. "Network-Centric Warfare: Its Origin and Future". *US Naval Institute Proceedings* 124, no. 1 (1998): 28-35.

Center, Microsoft Threat Intelligence. "Destructive Malware Targeting Ukrainian Organizations": Microsoft, 2022.

Center, Robert Strauss. "Strait of Hormuz: Assessing the Threat to Oil Flows through the Strait". University of Texas 2022.

Centre, Robert Strauss. "Strait of Hormouz - Iran Strikes First ": University of Texas 2022.

CERT-EU. "Airbus Supply Chain Hacked in Cyberespionage Campaign", edited by Computer Emergency Response Team (CERT) (EU), 2019.

CERT-UK. "Cyber Risks in the Supply Chain", edited by CERT-UK, 2015.

Chang, F.K. "Nato’s Baltic Defence Challenge". *Foreign Policy Research Institute* (7 June 2017).

Charlton, L.E.O. "The Menace of the Clouds". *The Aeronautical Journal* 42, no. 327 (1928): 288-98.

Checkel, J.T. . "The Constructivist Turn in International Relations Theory". *World Politics* 50, no. 2 (January 1998): 324-48.

Chee-Wooi, T, G. Manimanran, and Liu C. "Cybersecurity for Critical Infrastructures: Attack and Defense Modelling". *IEEE Transactions on Systems: System and Humans* 40, no. 4 (July 2010).

Chekinov, S. G. and Bogdanov, S. A. . "Прогнозирование Характера И Содержания Войн Будущего: Проблемы И Суждени". *Voennaya Mysl* (2019): 44-55.

Chen, D.D. . "Opening Statement of Mr David D. Chen Independent Analyst: Hearing before the Us China Economic and Security Review", edited by US Congress: Economic and Security Review Commission, 2017.

Cheney, R. "Mystique of Us Air Power." By E.A. Cohen (1994): 109-24.

Cheng, D. . "Taiwan’s F-16v Fighter Jet Purchase: Why It Matters". *The Heritage Foundation* (25 August 2020).

Cherepanov, A. and Lipovsky, R. . "Blackenergy – What We Really Know About the Notorious Attacks". *Virus Bulletin Conference* (October 2016).

Cheung, K. . "Cybersecurity in Logistics and Supply Chain Management: An Overview and Future Research Directions". *Institute of Transport and Logistics Studies* 146 (2021).

Chhabra, T., Haas, R. "Global China: Domestic Politics and Foreign Policy". *Brooking Institute* (September 2019).

Childs, N. "Hormuz Strait Tensions Highlight Naval Capability Challenges". International Institute for Strategic Studies 2019.

China, People's Republic of. "Anti-Secession Law", edited by National People's Congres, 2015.

———. "China’s Military Strategy of 2015", edited by The State Council Information Office of the People’s Republic of China, 2015.

———. "White Paper: China’s National Defense in the New Era", edited by The State Council, 2019.

"Chinese Hacking against Taiwan: A Blessing for the United States?". *The Diplomat* (23 January 2018).

Chong, A. . "Smart Power and Military Force: An Introduction". *Journal of Strategic Studies* 38, no. 3 (2015): 233-44.

Chris, C. . "Unmanned Deterrence: Deterring Terrorism with Armed Drones." SecBrief.org, https://www.secbrief.org/2013/05/unmanned-deterrence-deterring-terrorism-with-armed-drones/.

Churchill, W. "House of Commons Debate, 11 May 1953 at 3.32pm – Foreign Affairs", edited by Hansard, 1953.

———. "The Sinews of Peace (Iron Curtain Speech)." https://winstonchurchill.org/resources/speeches/1946-1963-elder-statesman/120-the-sinews-of-peace/.

———. "Tragedy of Europe Speech: Zurich, 19 September 1946." http://www.churchill-society-london.org.uk/astonish.html#:~:text=I9th%20September%201946.,about%20the%20tragedy%20of%20Europe.&text=If%20Europe%20were%20once%20united,hundred%20million%20people%20would%20enjoy.

Churchill, W. . "Conservative Mass Meeting: A Speech at Llandudno." In *Europe Unite Speeches 1947 and 1948* edited by R.S. Churchill, 416-18. London: Cassell, 1950.

Cieslak, E. "Air Defence of the Baltic States: Looking toward the Future". *Safety and Defence* 7, no. 2 (2021): 12-21.

Clapton, W. . "Risk in International Relations". *International Relations* 25, no. 3 (2011): 280-95:.

Clark, C. . "The Taiwan Relations Act and the U.S. Balancing Role in Cross-Strait Relations". *American Journal of Chinese Studies* 17, no. 1 (April 2010): 3-18.

Clarke, C. "Paths between Positivism and Interpretivism: An Appraisal of Hay's Via Media". *Politics* 29, no. 1 (2009): 28-36.

Clarke, R.A., and R.K. Knake. *Cyber War.* New York: Ecco, 2010.

Clausewitz, C. . *On War* New Jersey: Princeton University Press, 1832.

Clawson, P. "The Clinton Doctrine". *The Washington Institute for Near East Policy* December (1997).

Clayton, A. *The British Empire as a Superpower, 1919 - 39.* Georgia University of Georgia Press 1986.

Clinton, H. . "Transcript of Clinton's Confirmation Hearing to the Senate Foreign Relations Committee". *NPR* (13 January 2009).

Clinton, W.J. "The 1994 State of the Union Address", edited by Clinton Digital Library, 1994.

CNA. "National Defense Budget Was Greatly Increased to 358 Billion". (15 August 2019).

CNN. "2008 Georgia Russia Conflict – Fast Facts", *CNN Editorial Research*, 31 March 2020.

———. "Obama Says Us Has Asked Iran to Return Drone Aircraft", *CNN World*, 12 December 2011.

Coffey, L., Kochis, D. "Nato Summit 2021: Reinforcing Collective Defence in the Baltics". *The Heritage Foundation* (11 June 2021).

Cohen-Almagor, R. . "Internet History". *International Journal of Technoethics* 2, no. 2 (2011): 45-64.

Cohen, E. A. . "Mystique of Us Air Power". *Foreign Affairs* 73, no. 1 (1994): 109-24.

Cohen, R.S. "The Future of Warfare in 2030": RAND, 2020.

Cole, E. , and S. Ring. *Insider Threat: Protecting the Enterprise from Sabotage, Spying and Theft* Massachusetts: Elsevier, 2005.

Coleman, D. "U.S. Military Personnel 1954-2014", 2021.

Commission, 9/11. "The 9/11 Commission Report ": National Commission on Terrorist Acts Upon the United States 2004.

Committee, Senate Armed Servies. "Hearing to Recieve Testimony on Us Strategic Command and Us Cyber Command in Review of the Defense Request for Fiscal Year 2013 and the Future Years Defense Programe", edited by US Senate, 2012.

ComputerSecrity.com. "White Paper: Approaches to Usb Security ", 2020.

ComputerWeekly.com. "What Is Hypoconnectivity?" https://www.computerweekly.com/news/2240100953/What-is-hyperconnectivity.

Condliffe, J. B. . "Economic Power as an Instrument of National Policy". *The American Economic Review* 34, no. 1 (1944): 305-14.

Construct, International Maritime Security. "An International Approach", edited by IMSC, 2022.

Conway-Lanz, S. . "The Ethics of Bombing Civilians after World War Ii: The Persistence of Norms against Targeting Civilian in the Korean War". *The Asia-Pacific Journal* 12, no. 37 (2014).

Cooney, S. "Why Taiwan Is Not Hong Kong: A Review of the Prc's "One Country Two Systems" Model for Reunification with Taiwan ". *Washington Journal of Law* 6, no. 3 (1 July 1997): 497-548.

Cooper, Price Waterhouse. "Assessment of the Expected Economic Impact of the Tempest Programme (2021-2050)", 2021.

Cordesman, A.H. "America's Failed Strategy in the Middle East: Losing Iraq and the Gulf". *Center for Strategic and International Studies (CSIS)* (2 January 2020).

Cordesman, A.H. . "Syria's Uncertain Air Defence Capabilities". *Centre for Strategic and International Studies*, no. 6 May (2013).

Corera, G. "Inside a Us Military Cyber Team's Defence of Ukraine", *BBC News* 30 October 2022.

———. "Russia Hacked Ukrainian Satellite Communications, Officials Believe", *BBC News* 25 March 2022.

Cornish, P., R. Hughes, and D. Livingstone. "Cyberspace and the National Security of the United Kingdom: Threats and Responses". *A Chatham House Report* (March 2009).

Cornish, P., D. Livingstone, D. Clemente, and C. Yorke. "Cyber Security and the Uk's Critical National Infrastructure". *A Chatham House Report* (September 2011).

Council, Museum Directors. "Soft Power ", 2019.

Crawford, N.C. . "Just War Theory and the Us Counter Terror War". *Perspectives on Politics* 1, no. 1 (2003): 5-25.

Crowdy, T. . *The Enemy Within* London: Bloomsbury, 2011.

Crowther, G. A. . "The Cyber Domain". *The Cyber Defense Review* 2, no. 3 (2017): 63-68.

Croxton, D. . "The Peace of Westphalia of 1648 and the Origins of Sovereignty". *The International History Review* 21, no. 3 (1999): 569-91.

Csernatoni, R. . "Constructing the Eu's High-Tech Borders: Frontex and Dual-Use Drones for Border Management". *European Security* 27, no. 2 (2018): 175-200.

CSIS. "Significant Cyber Incidents since 2006": Centre for Strategic and International Studies (CSIS), 2020.

Cullen, P.J., and E. Reichborn-Kjennerud. "Understanding Hybrid Warfare". *Multinational Capability Development Campaign (MCDC)* (January 2017).

Cup, Tianfu. "Tfc - International Cyber Security Forum." http://www.tianfucup.com/en/#canjia.

Cyberwarzone. "New F-35 Jet Is Vulnerable to Cyber Attack", *Cyber-Security News*, 31 May 2014.

Cylance. "Op Cleaver ", 2014.

D'Urso, S. "Italy, United Kingdom and Sweden Sign Tempest Fcas Coordination Memorandum of Understanding". *The Aviationist* (5 January 2021).

———. "The U.S. Air Force Is Considering Buying New F-16 Aircraft", *The Aviationist* 1 February 2021.

D.A., Deptula. "Keeping 4th-Gen Fighters in the Game." By J.A. Tirpak. *Air Force Magazine* (1 October 2019).

Da Silva, F.A.B., D.F.C. Moura, and J.F. Galdino. "Classes of Attacks for Tactical Software Defined Radio". *International Journal of Embedded and Real-Time Communication Systems* 3, no. 4 (2012): 57-82.

Dahl, R.A. . "The Concept of Power". *Behavioural Science* 2, no. 3 (1957): 201-15.

Dalsjö, R., Berglund, C., Jonsson, M. . "Bursting the Bubble: Russian A2/Ad in the Baltic Sea Region". *Swedish Total Defence Research Institute* (March 2019).

Dalsjö, R., Jonsson, M., Norberg, J. "A Brutal Examination: Russian

Military Capability in Light of the

Ukraine War": International Insstitute for Strategic Studies 2922.

Daolio, A. . "Arab Allies Must Step up to Defend Freedom of Navigation in the Gulf". (9 August 2019).

Davenport, K. . "The Joint Comprehensive Plan of Action (Jcpoa) at a Glance": Arms Control Association 2022.

David, D. "Coronovirus: Uk Worst Hit among Major Economies", *BBC News Online*, 26 August 2020.

Davies, A. . "Putin: Nuclear Risk Is Rising, but We Are Not Mad", *BBC News*, 7 December 2022.

Davies, R. "Uk Unveils New Tempest Fighter Jet to Replace Typhoon", *The Guardian* 16 July 2018.

Davis, C.R. "Presentation to the Senate Armed Services Committee: Subcommittee on Tactical Air and Land Force", edited by Senate Armed Services Committee, 2014.

Davis, G.D. *Bombing the Axis Powers.* Alabama: Air University Press, 2006.

Davis, L.E., M. McNerney, and M.D. Greenbery. *Clarifying the Rules for Targeting and Killing* Santa Monica: RAND, 2016.

Davoodi, H., Clements, B., Schiff, J., Debaere, P. "Military Spending, the Pease Dividend, and Fiscal Adjustment". *IMF Staff Papers* 48, no. 2 (2001): 290-321.

DCDC. "Multi-Domain Integration ", edited by Ministry of Defence, 2020.

De Cerchio, R. . "Aircraft Systems Cyber Security", In *Digital Avionics Systems Conference (DASC)*, 2018.

Deane, P. . *The First Industrial Revolution* Cambridge Cambridge University Press, 1979.

Dear, K. . "Artificial Intelligence and Decision-Making". *The RUSI Journal* 164, no. 5 (29 November 2019): 18-25.

Deighton, A. . "Britain and the Three Interlocking Circles." In *Europe 1945-1990s: The End of an Era?*, edited by A. Varsori, 155-69. London: MacMillan), 1990.

Delbert, R.J., Rohozinski, R. and Crete-Nishihata, M. . "Cyclones in Cyberspace: Information Shapin and Denial in the 2008 Russia-Georgia War". *Security Dialogue* 43, no. 1 (2012): 3-24.

Dell. "Dell Annual Threat Report ", 2015.

Dempsey, M. "100% Right 0% of the Time: Why the Us Military Can't Predict the Next War " By M. Zenko. *Foreign Policy* (16 October 2012).

Dempsey, N. "Uk Defence Expenditure", edited by House of Commons Library, 2021.

Devanny, J., Martin, C., Stevens, T. "On the Strategic Consequences of Digital Espionage". *Journal of Cyber Policy* 6, no. 3 (15 November 2021): 429-50.

Dickinson, A. . "Spending Review: Reducing the 0.7% Aid Commitment", edited by House of Commons Library, 2020.

Dickson, B.J. "The Lessons of Defeat: The Reorganization of the Kuomintang on Taiwan, 1950-52". *The China Quarterly* 133 (1993): 56-84.

Dickson, J. "We Need a New Word for Cyber", *Dark Reading* 23 November 2015.

Dildy, D.C. . "The Air Battle for England: The Truth Behind the Failure of the Luftwaffe's Counter-Air Campaign in 1940". *Air Power History*, no. Summer (2016): 27-40.

Dockrill, S. . *Britain's Retreat from East Suez: The Choice between Europe and the World.* Basingstoke: Palgrave MacMillan, 2002.

Dougherty, C. "Confronting Chaos: A New Concept for Information Advantage ". *War on the Rocks* (9 September 2021).

Douhet, G. . *The Command of the Air.* Translated by D. Ferrari. Alabama: Air University Press, 1921.

Doyle, M.W. . "Kant, Liberal Legacies and Foreign Affairs". *Philosophy and Public Affairs* 12, no. 3 (1983): 205-35.

Dudney, R.S. "Douhet", *Air Force Magazine*, April 2021.

Duechars, R. . *The International Political Economy of Risk: Rationalism, Calculation and Power* London: Routledge, 2004.

Dueck, C. *Reluctant Crusaders: Power, Culture, and Change in American Grand Strategy.* Princeton Princeton University Press, 2006.

Duffin, E. "U.S. Defense Outlays and Forecast 2000-2031": Statistica, 2021.

Dunne, T. "The English School." In *The Oxford Handbook of Political Science* edited by R.E. Goodin. Oxford: Oxford University Press, 2011.

Dunstan, S. . *The Six Day War 1967: Sinai* London: Bloomsbury, 2012.

Dvilyanski, M. "Taking Action against Hackers in Iran": Meta, 2021.

Dyner, A.M. "Russia Beefs up Military Potential in the County's Western Areas". *The Polish Institute of International Affairs* (2019).

Easton, I. "Taiwan, Asia's Secret Air Power". *The Diplomat* (25 September 2014).

Eckhout, L. . "Is Moore's Law Slowing Down? What's Next?". *IEEE Computer Society*, no. July/August (2017).

Economist-Intelligence-Unit. "Cyber Power Index": Booz Allen Hamilton 2011.

Editor. "How a Rising China Remade Global Politics ". *World Politics Review* (26 January 2022).

Editorial. "F-16v Still Taiwan's Greatest Hope When Dealing with China's "Strongest Dragon" J-20". *Defence View* (13 January 2022).

———. "Pla Report Sobering, but Accurate", *Taipei Times*, 3 September 2021.

Edmonds, M, Tsai, M.M. *Defending Taiwan: The Future Vision of Taiwan's Defence Policy and Military Strategy.* New York: Routledge, 2003.

Eisenhower-Group. "Open Letter: Opposition to Nato Expansion". *Arms Control Association* (26 June 1997 1997).

Elbaum, B., Lazonick, W. "The Decline of the British Economy: An Institutional Perspective". *The Journal of Economic History* 44, no. 2 (1984): 567-83.

Electric, General. "Military Engines ", 2022.

Ellison, R. . "Left of Launch". *Missile Defence Advisory Alliance*, no. 16 March (2015).

Ellwood, T. . "Ministry of Defence Computers: Written Question - 141014", In *Written Questions and Answers*, edited by UK Parliament, 2018.

EMEA. "Aviation: Satellite Services", edited by Middle East and Africa (EMEA) Satellite Operators Association (ESOA) Europe, 2020.

Eroukhmanoff, C. . "Securitisation Theory." In *International Relations Theory* edited by S. McGlinchey, R. Walters and C. Scheimpflug. Bristol E-International Relations Publishing, 2017.

Ervural, B.C., and B. Ervural. "Overview of Cyber Security in the Industry 4.0 Era." In *Industry 4.0: Managing the Digital Transformation* edited by A. Ustundag and Cevikcan. E., 267-84. Birmingham: Springer, 2019.

EurAsianDesk. "From Ladakh to South China Seas, Us Deploys Its 'Most Lethal' Armed Drone to Check Chinese Machoism", *Eurasian Times*, 30 September 2020.

Europe, Council of. "Statute of the Council of Europe", 1949.

Evans, G., and M. Sahnoun. *International Commission on Intervention and State Sovereignty (Iciss), the Responsibility to Protect* Ottawa: International Development Research Centre, 2001.

Evans, M., L. A. Maglaras, Y. He, and H. Janicke. "Human Behaviour as an Aspect of Cybersecurity Assurance". *Security and Communications Networks* 9 (2016): 4667-79.

Exeter, University of. "Research Ethics Policy and Framework", 2021.

Export, Rosoboron. "Avtobaza-M Air Defence System ", 2022.

Ezrow, N. . *Global Politics and Violent Non-State Actors* London: Sage Publications, 2017.

F-Secure. "Worm:W32/Agent.Btz'", In *Threat Descriptions* 2022.

Fabian, S. . "The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy". *Defense and Security Analysis* 35, no. 3 (2019): 308-25.

Falk, R. . "Revisiting Westphalia, Discovering Post-Westphalia". *Journal of Ethics* 6, no. 4 (2002): 311-52.

Farley, R. "Is China Rethinking the Shenyang J-31 Fighter?", *The Diplomat*, 13 November 2018.

Farley, R. . "Theft Can't Help China's Air Force Build Quality Engines". *The National Interest* (11 December 2021).

Farmer, B. . "Troops Leaked Confidential Data on Twitter and Facebook", *The Telegraph*, , 8 July 2018.

Federation, Russian. "Strategy for the National Security of the Russian Federation up to 2020", edited by Government of the Russian Federation, 2009.

———. "Us Cyber Attack on Fan: Details of the Failed Operation Us Cyber Command", edited by Federal News Agency, 2019.

Fehrenbach, T.R. . *This Kind of War: The Classic Military History of the Korean War* Dulles: Potomac Books, 2008.

Feinstein , D. "Indictment: Iranians Made 'Coordinated' Cyberattacks on U.S. Banks, Dam." By J. Marks. *Politico* (24 March 2016).

Fielding, J. . "The People Problem: How Cyber Security’s Weakest Link Can Become a Formidable Asset". *Computer Fraud and Security* 6 (1 January 2020): 6-9.

Finkle, J. . "Exclusive: Iran Hackers May Target U.S. Energy, Defense Firms, Fbi Warns", *Reuters* 13 December 2014.

Firepower, Global. "2022 Taiwan Military Strength ": Global Firepower 2022.

Fishel, R., and A. Stein. "Lessons Learned from the Air War against the Islamic State", *War on the Rocks*, 23 February 2018.

Flibbert, A. . " The Road to Baghdad: Ideas and Intellectuals in Explanations of the Iraq War". *Security Studies* 15, no. 2 (2006): 310-52.

Flockhart, T. . "Constructivism and Foreign Policy." In *Foreign Policy*, edited by S. Smith, 79-94. Oxford Oxford University Press, 2008.

Focarelli, C. "The Responsibility to Protect Doctrine and Humanitarian Intervention: Too Many Ambiguities for a Working Doctrine". *Journal of Conflict and Security Law* 13, no. 2 (2008): 191-213.

Fontanella-Kahn, J., and S. Pfeifer. "United Technologies-Raytheon Deal Creates Aerospace Powerhouse", *Financial Times*, 10 June 2019.

Foolath, V.E., and H. Stark. "How Israel Destroyed Syria’s Al Kibar Nuclear Reactor", *Das Spiegel International*, 2 November 2009.

Force, Royal Air. "Reaper (Mq09a)", edited by Royal Air Force, 2022.

Forde, S. . "Varieties of Realism: Thucydides and Machiavelli". *The Journal of Politics* 54, no. 2 (1992).

Fortinet. "Independent Study Pinpoint Significant Scada/Ics Security Risks", 2019.

Forum, Information Security. "Methodology 2 (Iram2)", 2019.

Foster-Wallace, D. . "This Is Water". *Commencement Speech to Kenyon College, Ohio* (2005).

Fowler, M. R., and J. M. Bunck. *Law, Power, and the Sovereign State: The Evolution and Application of the Concept of Sovereignty* Pennsylvania: Pennsylvania State University Press, 1995.

Foxall, A. "Putin Sees and Hears It All: How Russia's Intellgience Agencies Manace the Uk". *Henry Jackson Society* (November 2018).

Franklin, J.K. "The Hollow Pact: Pacific Security and the Southeast Asia Treaty Organization." Texas Christian University, 2006.

Frankum, R. . *Like Rolling Thunder: The Air War in Vietnam, 1964-1975.* Vol. 3, New York Rowman & Littlefield, 2005.

Frantzman, S.J. . "Iran Claims Its Air Defense Confronted Two Us Drones During Recent Drill", *Jerusalem Post*, 9 November 2021.

Frederking, B. " Constructing Post-Cold War Collective Security". *American Political Science Review* 97 (2003): 363-78.

Freeberg, S. "Top Official Admits F-35 Stealth Fighter Secrets Stolen", *Breaking Defence*, 20 June 2013.

Freeman, C., T. Hill, A. McKenna, S. Papa, and M. White. "Measuring Diplomatic Capacity as a Source of National Power". *Review of International Affairs* 40, no. 1 (2020): 5-17.

Freund, E. "Freedom of Navigation in the South China Sea: A Practical Guide". *Belfer Center* (June 2017).

Frum, D. "The Enduring Lessons of the 'Axis of Evil' Speech". *The Atlantic* (29 January 2022).

Fulghum, D. . "Areas Blog (April 2007)", *Aviation Weekly*, April 2007.

Fund, International Monetary. "World Economic Outlook: The Great Lockdown", 2020.

Futter, A. . "Cyber Semantics: Why We Should Retire the Latest Buzzword in Security Studies". *Journal of Cyber Policy* 3, no. 2 (2018): 201-16.

———. "The Dangers of Using Cyber Attacks to Counter Nuclear Threats". *Arms Control Today* 46, no. 6 (July/August 2016).

———. "Hacking the Bomb: Nuclear Weapons in the Cyber Age", In *ISA Annual Conference*. New Orleans, 2015.

Gaddis, J.L. "Toward the Post-Cold War World ". *Council on Foreign Relations* 70, no. 2 (1991): 102-22.

Gady, F. "Taiwan Wants the F-35 Stealth Fighter". *The Diplomat* (21 March 2018).

Gady, F. . "China's First Fifth Generation Fighter Jet Is Operations". *The Diplomat* (2 October 2017).

Gady, F.S. . "New Snowdon Documents Reveal Chinese Behind F-35 Hack", *The Diplomat*, 27 January 2015.

Galeotti, M. "The 'Gerasimov Doctrine' and Russian Non-Linear War ". In Moscow's Shadows 2014.

Galeotti, M. . "The Gerasimov Doctrine". *Berlin Policy Journal* (28 April 2020).

Gang, Q. "Obama Says Us Will Defend Japan in Island Dispute with China." By J. McCurry, Branigan, T. *The Guardian* (24 April 2014).

Garbarino, M. . "F-16 Service Life Extension Program a 'Great Deal' for Department of Defense, Taxpayers", edited by United States Air Force Materiel Command, 2018.

Gardner, F. "First Joint Naval Exercise by Israel and Gulf States Signals Iran Worries", *BBC News*, 15 November 2021.

———. "Mercer Street: Tanker Blast Evidence Points to Iran, Says Us", *BBC News* 7 August 2021.

———. "Why Iran's Capture of Us Drone Will Shake Cia", *BBC News* 8 December 2011.

Garg, A.K. . "Fourth Generation Systems and New Wireless Technologies." In *Wireless Communications and Networking*, edited by A.K. Garg. Burlington: Morgan Kaufmann, 2007.

Gates, R. . "Speech to the Us Military Academy, West Point ", edited by US Department of Defense, 2011.

Gatopoulos, A. . "The Nagorono-Karaback Conflict Is Ushering in a New Age of Warfare", *Aljazera Online*, 11 October 2020.

Geers, K. . "The Ruthless Russian Hacking Unit That Tried to Crash Ukraine." By D. Templeton-Raston (26 December 2019).

Gerasimov, V. . "The Value of Science Is in the Foresight". *Military Review* (January 2016): 23-29.

———. "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations'". *Military-Industrial Kurier* (27 February 2013).

Ghafir, I. . "Security Threats to Critical Infrastructure: The Human Factor". *The Journal of Supercomputing* (26 March 2018): 1-17.

Ghasmekhani, H., D. Soule, and G. S. Westerman. "Competitive Advantage in a Digital World: Toward an Information-Base View of the Firm": SSRN, 2015.

Gibson, W. *Neuromancer* New York: Ace, 1984.

Giles, K. "'Information Troops: A Russian Cyber Command?". *3rd International Conference on Cyber Conflict* (2011).

Giles, K. and Seaboyer, A. . "The Russian Information Warfare Construct". *Defence Research and Development Centre Canada* (March 2019).

Gilpin, R. . *War and Change in World Politics* Cambridge Cambridge University Press, 1981.

Gladius, M. . "What Is an Expeditionary Force? No, Really, What Is It?". *Small Wars Journal* (13 February 2020).

Gladstone, R. . "Iran Is Asked to Return Us Drone'", *New York Times*, 12 December 2011.

Gladwell, M. *The Bomber Mafia.* London: Penguin Books, 2021.

Glass, A. "President Bush Cites 'Axis of Evil,' Jan. 29, 2002". *Politico* (29 January 2019).

Gleicher, N. "Iranian Hackers Targeted Western Militaries". *United States Peace Institute* (16 July 2021).

"Global Economy Watch: Prediction for 2021". PWC, 2021.

Goddard, S. . "When Right Makes Might: How Prussia Overturned the European Balance of Power". *International Security* 33 (2009): 110–42.

Goldberg, L.R. . "The Structure of Phenotypic Personality Traits". *American Psychologist* (January 1993): 26-34.

Goldfein, D. "Us Air Force General: No Pause in Drone Operations Amid Iran Tension." By V. Insinna. *Defence News* (27 June 2019).

Goldie, A. . "Joint Strike Fighter Aircraft: Question for Ministry of Defence", edited by UK Parliament. Written Questions, Answers and Statements, 2020.

Goldman, A., and J. E. Barnes. "Air Force Defector to Iran Severely Damaged Us Intelligence Efforts, Ex-Officials Say", *The New York Times*, 15 February 2019.

GoldSparrow. "Barium Group Threatens Millions of Computers through Stealthy Supply Chain Hacking Attacks": EnigmaSoft, 2020.

Golkar, S. . "Iran's Intelligence Organizations and Transnational Suppression". *The Washington Institute for Near East Policy* (5 August 2021).

Gomez, J. "China Coast Guard Uses Water Cannon against Philippine Boats", *ABC News*, 18 November 2021.

Gomez, O., and D. Gasper. "Human Security", edited by UNDP Human Development Report Office: United Nations 2020.

Gompert, D.C., Cevallos, A., Garafola, C.L. . "War with China: Thinking the Untinkable ". *RAND* (2016).

Gould, J. . "A Company Made a 4.436% Profit on a Cheap Part Sold to the Pentagon", *Defence News*, 15 May 2019.

Gowland, D., Turner, A. . *Britain and European Integration 1945-1998: A Documentary History* New York Routledge, 2010.

Gramer, R. "Russia's Stripped Its Western Borders to Feed the Fight in Ukraine", *Foreign Policy*, 28 September 2022.

Granova, A., and M. Slaviero. "Cyber Warfare." In *Computer and Information Security Handbook*, edited by J.R.   Vacca. Burlington: Morgan Kaufmann, 2017.

Gray, C.S. *Hard Power and Soft Power: The Utility of Military Force as an Instrument of Policy in the 21st Century.* Pennsylvania: US Army War College, 2011.

Grazier, D. . "F-35 Officials Prove Need for Cyber Testing by Cancelling One", In *Project on Government Oversight*: Centre for Defence Information, 2015.

Grazier, D., and M. Smithburger. "Pentagon Testing Office Calls Foul on F-35 Operational Testing", In *Project on Government Oversight*: Centre for Defence Information, 2015.

Greenberg, A. "The Full Story of the Stunning Rsa Hack Can Finally Be Told", *Wired*, May 2021.

———. "A Mysterious Hacker Group Is on a Supply Chain Hijacking Spree", *Wired* 3 May 2019.

———. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* New York: Anchor Books 2020.

———. "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History", *Wired* 17 October 2018.

Greenberg, A. . "How an Entire Nation Became Russia's Test Lab for Cyberwar", *Wired*, 28 June 2017.

Greenert, J.W., and R.T. Odierno. "Memorandum for the Secretary of Defense: Adjusting the Ballistic Missile Defense Strategy", edited by US Department of Defense, 2014.

Grey, C. S. *Modern Strategy* Oxford: Oxford University Press, 1999.

Grey, C. S., and G. Sloan. *Geopolitics, Geography and Strategy* London: Routledge, 2013.

Grimal, F., and J. Sundram. "Combat Drones: Hives, Swarms and Autonomous Action". *Journal of Conflict and Security Law* 23, no. 1 (2018): 105-35.

Gross, J.A., and T. Staff. "Idf Launches Airstrikes against Iranian Quds Force in Syria", *The Times of Israel*, 14 November 2020.

Gross, L. . "The Peace of Westphalia, 1648-1948". *American Journal of International Law* 42, no. 1 (1948): 20-41.

Group, International Crisis. "10 Conflicts to Watch in 2022": International Crisis Group, 2022.

Gunzinger, M. "Building the Future Force". *Air Force Magazine* (26 March 2021).

Gunzinger, M. Autenrief, L. . "Building a Force That Wins: Recommendations for the 2022 Nationl Defense Strategy ": The Mitchell Institute for Aerospace Studies 2021.

Guzzini, S. . "A Reconstruction of Constructivism in International Relations". *European Journal of International Relations* 6, no. 2 (147-182 2000).

Haakonssen, K. . "Hugo Grotius and the History of Political Thought". *Political Theory* 13, no. 2 (1985): 239-65.

Haas, R.N. "Enlarging Nato: A Questionable Idea Whose Time Has Come ". *Brooking Institute* (1 March 1997 1997).

Haass, R. . "The Age of Nonpolarity". *Foreign Affairs* (May/June 2008): 44-56.

Habiger, E. . "United States. United States Senate, Hearings before the Committee on Armed Services: Strategic Forces", edited by Committee on Armed Services. United States United States Senate, 1997.

Hadley, G. "Hacking the Supply Chain ", *Air Force Magazine*, 3 December 2021.

Haipeng, Z., Guoqiang, L. "The Treaty of Shimonoseki, the Diaoyu Islands and the Ryukyu Issue". *International Critical Thought* 7, no. 1 (20 March 2017): 93-108.

Haizler, O. "The United States’ Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking". *Cyber, Intelligence and Security* 1, no. 1 (2017).

Hajnal, P.I. *The G8 System and the G20 Evolution, Role and Documentation* London: Routledge, 2019.

Hakala, J., Melnychuk, J. "Russia’s Strategy in Cyberspace". *NATO Cooperative Cyber Defence Centre of Excellence* (June 2021).

Hall, R. . "Isis Caliphate Defeated: How Did It Happen and Do They Still Pose a Threat?", *Independent*, 23 March 2019.

Hallion, R.P. . *Storm over Iraq: Air Power and the Gulf War* London: Smithonian Books, 1997.

Hamilton, T., Ochmanek, D. . "Operating Low-Cost, Reusable Unmanned Aerial Vehicles". *RAND* (2020).

Hamin, Z. . "Insider Cyber-Threats: Problems and Perspectives". *International Review of Law, Computers and Technology* 14, no. 1 (2000): 105-13.

Hamrah, S., Eliasen, A. . "The China-Iran Strategic Partnership: 40 Years in the Making". *The Diplomat* (4 December 2021).

Hanson, F. "Cyber Maturity in the Asia Pacific Region 2017": Australian Strategic Policy Institute 2018.

Haradhan, M. . "The Second Industrial Revolution Has Brought Modern Social and Economic Developments". *Journal of Social Sciences and Humanities* 6, no. 2 (2020): 1-14.

Harding, L. . "How Edward Snowdon Went from Loyal Nsa Contractor to Whistle Blower", *The Guardian*, 1 February 2014.

Harford, T. . "Crash: How Computers Are Setting Us up for Disaster", *The Guardian*, 11 October 2016.

Harknett, R.J., Smeets, M. . "Cyber Campaigns and Strategic Outcomes". *Journal of Strategic Studies* (4 March 2020).

Harnisch, S., C. Frank, and H.W. Mauli. *Role Theory in International Relations: Approaches and Analyses* London: Routledge, 2011.

Harper, C., Lawrence, T., Sakkov, S. "Air Defence of the Baltic States". *International Centre for Defence and Security* (May 2018).

Harper, J. "Air Force's Ngad Program 'Progressing Per Plan'", *National Defense* 21 September 2021.

———. "Spending on Drones Projected to Soar", *National Defence*, 15 March 2019.

Harrington, D.F. "The Berlin Blockade Revisited". *The International History Review* 6, no. 1 (1984).

Harris, B.F. "United States Strategic Culture and Asia-Pacific Security". *Contemporary Security Policy* 35, no. 2 (2014): 290-309.

Harrison, T., K. Johnson, and T. G. Roberts. "Space Threat Assessment 2018": Centre for Strategic and International Studies, 2018.

Hart, C. . "Hackers Target Airbus Suppliers". *Supply Management* (27 September 2019).

Hart, J. . "Three Approaches to the Measurement of Power in International Relations". *International Organisation* Spring (1976): 289-305.

Hartmann, K., and K. Giles. "Uav Exploitation: A New Domain for Cyber Power", In *8th International Conference on Cyber Conflict*, 205-22: NATO CCDCOE 2016.

Hartmann, K., and C. Steup. "The Vulnerability of Uavs to Cyber-Attacks; an Approach to the Risk Assessment", In *Cyber Conflict (CyCon) 5th International Conference*, 1-23, 2013.

Harvey, N. . "Information Troops: A Russian Cyber Command?" By K. Giles. *3rd International Conference on Cyber Conflict* (2011).

Hashim, A.S., Patte, G. . "“What Is That Buzz?” the Rise of Drone Warfare". *Counter Terrorist Trends and Analysis* 4, no. 9 (2012): 8-13.

Hassan, D. "Rise of Territorial State and the Treaty of Westphalia". *Yearbook of New Zealand Jurisprudence* (2006): 62-70.

Hassan, H. . "The True Origins of Isis", *The Atlantic*, 2018.

Hassanzadeh, A., Rasekh, A, Galelli, S. . "A Review of Cybersecurity Incidents in the Water Sector". *Journal of Environmental Engineering* 146 (Jul 2020).

Hathaway, M. . "Cyber Readiness Index 2.0: A Plan for Cyber Readiness": Potomac Institute for Policy Studies, 2015.

Hausken, K., and J. W. Welburn. "Attack and Defense Strategies in Cyber War Involving Production and Stockpiling of Zero-Day Cyber Exploits". *Information System Frontiers* (September 2020).

Havel, L. "Speech to the Czech and Slovak Federal Assembly on Thursday 10 May 1990", edited by Czech and Slovak Federal Assembly. Council of Europe (Speeches) 1990.

Havercroft, J. . "Was Westphalia ‘All That’? Hobbes, Bellarmine, and the Norm of Non-Intervention". *Global Constitutionalism* 1, no. 1 (2012): 120-40.

Hawksworth, J., Clarry, R., Audino, H. . "The Long View: How Will the Global Economic Order Change by 2050?": PWC, 2017.

Heappey, J. "New British Plan Looks to Boost F-35 Numbers, but Is It Still Aiming for 138?" By A. Mehta. *Defence News* (23 March 2021).

Heath, R. "Britain Braces for Not-So-Special Relationship with Biden", *Politico* 31 December 2020.

Heickero, R. . "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations". *Swedish Defence Research Agency* (March 2010).

Hemsley, K.E., Fisher, R.E. "History of Industrial Control System Cyber Incidents ": US Department of Energy 2018.

Henley, S., R. Currer, B. Scheuren, A. Hess, and G. Goodman. "Autonomic Logistics - the Support Concept for the 21st Century’", In *Aerospace Conference* 417-21, 2000.

Hill, C. "What Next for British Foreign Policy in a Post-Brexit World?", *The Guardian*, 18 August 2019.

Hille, P. "F-35: Why Germany Is Opting for the Us-Made Stealth Fighter Jet". *DW* (16 March 22 2022).

Hilley, S. . "Uk Ministry of Defence Cracks Down on Ut Security after Theft of Laptop’". *Computer Fraud and Security* 3 (2008): 2-3.

Hillier, S. "Royal Air Force Strategy: Delivering a World-Class Air Force " By Royal Air Force (2017).

Hitchens, T. . "New Joint Warfighting Plan Will Help Define ‘Top Priority’ Jadc2: Hyten", *Breaking Defense* 29 January 2021.

HMG. "Collection: Global Britain – Delivering on Our International Ambition ". Gov.UK, 2017.

———. "Imperial Conference 1926 – Inter-Imperial Relations Committee: Report, Proceedings and Memoranda (the London Declaration)", edited by Commonwealth. London 1926.

Hoa, R. "Rhetoric of Responsibility: R2p’s Harmful Application in Humanitarian Practice". *E-International Relations* (15 February 2015).

Hobbes, T. *Leviathan* London: Penguin, 1651.

Hochberg, J. G., K. A. Jackson, J. F. McClary, and D. D. Simmonds. "Addressing the Insider Threat", In *The DOE Computer Security Group Conference*, 1993.

Hodgson, Q. E., L.. Ma, K. Marcinek, and K. Schwindt. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace* Santa Monica: RAND, 2019.

Hoffmann, S. . *The Political Ethics of International Relations* New York: Carnegie Council on Ethics and International Affairs, 1988.

Holsti, K. "National Role Conceptions in the Study of Foreign Policy". *International Studies Quarterly* 14 (September 1970): 233-309.

Holt, R. "Sandworm: A Tale of Disruption Told Anew", *We Live Security*, 21 March 2022.

Homolar, A. . "Rebels without a Consciences: The Evolution of the Rogue States Narrative in Us Security Policy". *European Journal of International Relations* 17, no. 4 (2010): 705-27.

Homoliak, I., F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa. "Insight into Insiders and It: A Survey of Insider Threat Taxonomies, Analysis, Modelling and Countermeasures". *ACM Computing Surveys* 99 (2019): 1-40.

Hood, C., and D.K.C. Jones. *Accident and Design – Contemporary Debates in Risk Management.* London: Routledge Taylor and Francis Group, 1997.

Hopf, T. "The Promise of Constructivism in International Relations Theory". *International Security* 23, no. 1 (1998).

Horschig, D. . "Cyber-Weapons in Nuclear Counter-Proliferation". *Defense and Security Analysis* 36, no. 3 (2020).

Horton, C. "Taiwan's Status Is a Geopolitical Absurdity". *The Atlantic* (8 July 2019).

Huan, A., Hui, T.M. "Kinmen at a Crossroads: A Balancing Act? ": Rajaratnam School of International Sudies 2019.

Humphrey, T. . "Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil Gps Spoofing", edited by Investigations Submitted to the Subcommittee on Oversight, and Management of the House Committee on Homeland Security: US Congress 2012.

Hung-wei, Chien. "How Taiwan Is Trying to Defend against a Cyber 'World War Iii'." By E. Cheung, Ripley, W.. Tsai, G. . *CNN Business* (24 July 2021).

Hunt, J. "Foreign Secretary Hunt: Britain's Role in a Post-Brexit World", edited by FCO. Gov.UK, 2019.

———. "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed", edited by Gov.UK Press Release, 2018.

Hunzeker, M.A. "Taiwan's Defense Plans Are Going Off the Rails ". *War on the Rocks* (18 November 2021 2021).

Hyde-Price, A. "Nato and the Baltic Sea Region ". *NATO Research Fellowship* (2000).

Hysolate. "Sandbox Software Development: Use Cases and Techniques ": Hysolate, 2022.

Hyten, J. "Joint Cheifs of Staff Vice Chair on Defence Technology ", *Emerging Technology Institute* 26 July 2021.

IAEA. "Implementation of the Npt Safeguard Agreement in the Syrian Arab Republic": International Atomic Energy Agency 2011.

IATA. "Aviation Cyber Security": International Air Transport Association 2020.

IBM. "Cost of Insider Threats Report 2020 ": IBM, 2020.

ICAO. "Airspace Sovereignty", In *ICAO Worldwide Air Transport Conference*, 2013.

———. "Chicago Convention on International Civil Aviation": International Civil Aviation Authority 1944.

———. "Civil Aviation Cyber-Security ": International Civil Aviation Authority 2020.

ICRC. "The Geneva Conventions of 1949 and Their Additional Protocols": International Committee of the Red Cross, 2014.

Igarashi, T. "When Did the Roc Abandon “Retaking the Mainland”? The Transformation of Military Strategy in Taiwan". *Journal of Contemporary East Asia Studies* 10, no. 1 (2021): 136-55.

Igure, V.M., S.A. Laughter, and R.D. Williams. "Security Issues in Scada Networks". *Computers and Security* 25, no. 7 (2006): 498-506.

Ilascu, I. . "The Airborne Threat of Software-Defined Radio Attacks", In *Bitefender Box* 2017.

Inhofe, J. "Praise Senate Passage of National Defense Authorization Act for Fiscal Year 2022." news release, 15 December, 2021, https://www.armed-services.senate.gov/press-releases/reed-inhofe-praise-senate-passage-of-national-defense-authorization-act-for-fiscal-year-2022.

Iran, Islamic Republic of. "Constitution of the Islamic Republic of Islam ", edited by Islamic Parliament of Iran, 1979.

Ireland. "Air Corps", edited by Irish Defence Forces, 2023.

ISO. "Iso Guide 73: 2009 – Risk Management (Vocabulary) ", 2009.

———. "Iso/Ie 27005:2011 – Information Security Risk Management", 2011.

ITU. "Global Cybersecurity Index, Version 4 ": International Telecommunications Union 2018.

J.H., Matlary. *Hard Power in Hard Times.* London: Palgrave Macmillan, 2018.

J.J., Mearsheimer. *The Tragedy of Great Power Politics* New York: Norton Publishing Company, 2001.

Ja, A. . "Insider Vs. Outsider Threats". *Infosec* (8 June 2015).

Jablonsky, D. . "National Power". *Parameters* Spring (1997): 34-54.

Jackson, P.T., and D.H. Nexon. "Constructivist Realism or Realist-Constructivism". *International Studies Review* 6 (2004): 337-52.

———. "Whence Casual Mechanisms? A Comment on Legro". *Dialogue IO* 1, no. 1 (2002): 81-101.

Jackson, R. . *Sovereignty: The Evolution of an Idea* Cambridge: Polity Press, 2007.

Jackson, R.H. . "Pluralism in International Relations". *Review of International Studies* 18, no. 3 (July 1992): 271-81.

Jafari, S. "Iran's Middle East Influence May Actually Be Declining". *Atlantic Council* (5 November 2021).

Jaincke, M., and K.H. Jacob. "A Third Industrial Revolution." In *Long-Term Governance for Social-Ecological Change* edited by K. Eisenack and K.H. Jacob, 47-70. Abingdon: Routledge, 2013.

Jalil, Z. "China Sends 30 Warplanes into Taiwan Air Defence Zone", *BBC News* 31 May 2022.

Japan. "Statistics on Scrambles through the First Quarter of Fy2019", edited by Japan Ministry of Defence - Joint Staff Press Release, 2019.

———. "Treaty of Mutual Cooperation and Security between Japan and the United States of America ", edited by Japan Ministry of Foreign Affairs, 1990.

Jarvis, D.S.L., and M. Griffiths. "Risk and International Relations: A New Research Agenda?". *Global Society* 21, no. 2 (2007): 1-4.

Jeffery, R. *Hugo Grotius in International Thought* New York: Palgrave MacMillan, 2006.

Jennings, G. "Raf to Expand Swarming Drone Capabilities'". *Janes* (14 July 2021).

———. "Uk Defence Command Paper: Raf to Axe Older Typhoons". *Janes* (22 March 2021).

———. "Uk Receives New Reaper Uav to Support Transition to Protector". *Janes* (5 November 2021).

Jennings, N. . "Deterring Chinese Aggression". *Small Wars Journal* (1 March 2016).

Jie, Y., Wallace, J. "What Is China's Belt and Road Initiative ". *Chatham House* (16 September 2021).

Joe, R. "Anatomy of a Taiwan Invasion: The Air Domain". *The Diplomat* (3 April 2019).

———. "Beyond China’s J-20 Stealth Fighter". *The Diplomat* (20 September 2019).

———. "How the Descendants of a 1950s Bomber Transformed China’s Strike Reach". *The Diplomat* (18 November 2020).

John, P.O., S.E. Hampson, and L.R. Goldberg. "The Basic Level in Personality-Trait Hierarchies: Studies of Trait Use and Accessibility in Difference Contexts". *Journal of Personality and Social Psychology* 60, no. 3 (1991): 348-61.

Johnson, A.L. . *Wars in Peace: British Military Operations since 1991* London: RUSI, 2014.

Johnson, A.M., Axinn, S. . "The Morality of Autonomous Robots". *Journal of Military Ethics* 12, no. 2 (2013).

Johnson, B. "Chinese Hackers Used Microsoft Browser to Launch Google Strike", *The Guardian* 15 January 2010.

———. "What Can the Uk Do Now after Russia Is Linked to Spy Attack." By J. Lawless. *PBS* (13 March 2018).

Johnson, B. . "Boris Johnson Once Compared Hillary Clinton to ‘as Sadidistic Nurse in a Mental Hospital." By R. Sanchez (10 February 2015).

———. "Foreign Secretary Announces 250 New Diplomatic Roles and Ten New Sovereign Missions", edited by Gov.UK. Gov.UK, 2018.

———. "Uk and America Can Better Friends Than Even Mr Obama…If We Leave the Eu", *The Sun* 22 April 2016.

Johnson, D.E. . "An Overview of Land Warfare": The Heritage Foundation 2018.

Johnson, J. . "Cyber Pearl Harbour Versus the Real Pearl Harbor." By R. Steinnon (7 December 2017).

Johnson, J. , and P. Robison. "Boeing Is Killing It by Squeezing Its Suppliers". *Bloomberg Businessweek* (14 February 2018).

Johnson, L. . *Security Controls Evaluation, Testing and Assessment Handbook.* Amsterdam: Elsevier.

Joiner, K. F., A.. Ghildyal, A.J. Laing, and N. Devine. "Four Testing Types Core to Informed Ict Governance for Cyber-Resilient Systems". *International Journal of Advances in Security* 11, no. 3 (2018): 313-27.

Jones, B. . "Global China: Assessing China's Growing Role in the World." By Brookings Institute (2021).

Jones, G. *Multinationals and Global Capitalism* Oxford: Oxford University Press, 2005.

Jones, S. "Russia’s Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare": Center for Strategic and International Studies 2022.

Jost, S. "Back Door for Hackers? F-35 Cyber Weaknesses in the Spotlight." By Staff Writter. *Global DEefence.com* (March 2019).

Journalism, Bureau of Investigative. "Hc 772 Defence Committee: Written Evidence from the Bureau of Investigative Journalism", edited by UK Parliament. Parliamentary Business 2014.

Kainikara, S. . "The Strategy of Deterrence and Air Power". *Royal Australian Air Force, Air Power Development Centre* (2008).

Kallas, K. "Estonia’s Pm Says Country Would Be ‘Wiped from Map’ under Existing Nato Plans." By R. Milne. *Financial Times* (22 June 2022).

Kaminski, J. . "Rethinking Realism and Constructivism through the Lenses of Themes and Ontological Primacy - Introduction-Integrative Pluralism and

21st Century International Relations Theorising". *Croatian International Relations Review* (November 2019).

Kang, D. . "Guardians of the Homeland: Looming Threats to the Air Alert Mission", *War on the Rocks*, 6 June 2016.

Kapan, C. . "Air Power’s Visual Legacy: Operation Orchard and Aerial Reconnaissance Imagery as Resus De Geurre". *Critical Military Studies* 1, no. 1 (2015): 61-78.

Kaplan, F. *Dark Territory: The Secret History of Cyberwar* New York Simon and Schuster, 2016.

Kaspersky. "Bad Rabbit Ransomware". *Kaperskylabs: Secure List* (24 October 2017).

———. "What Is Spear Phishing? ", 2020.

Katz, M.N. "Great Power Clashes Will Reshapte America ". *National Interest* (7 August 2021).

Katzman, K., Nerurkar, N. "Iran’s Threat to the Strait of Hormuz ", edited by Congressional Research Service, 2012.

Keck, Z. "Engine Problems: Why China's J-20 Stealth Fighter Can't Beat America's F-22 or F-35". *The National Interest* (8 July 2020).

Keck, Z. . "The Hard Side of Soft Power", *The Diplomat*, 24 July 2013.

Keenan, G.F. "A Fateful Error", *The New York Times*, 5 February 1997 1997.

Keenes, E. . "Paradigms of International Relations: Bringing Politics Back In". *International Journal of Advances in Security* 44, no. 1 (1989): 41-67.

Keller, J. "Iran–U.S. Rq-170 Incident Has Defense Industry Saying 'Never Again' to Unmanned Vehicle Hacking". *Military-Aerospace Electronics* (3 May 2016).

Kelley, M. "The Imperative to Field a Cutting-Edge Air Force", *Defense News*, 26 July 2021.

Kelley, M. . "Nsa: Snowden Stole 1.7 Million Classified Documents and Still Has Access to Most of Them", *Business Insider*, 13 December 2013.

Kelly, J. "George Hw Bush: What Makes a One-Term President?", *BBC News* 2 December 2018.

Kelly, T.K., J. Dobbins, B. Sude, and B. Connable. *Knowing the Enemy* Santa Monica: RAND, 2017.

Kemp, H.C. . "Left of Launch: Countering Theatre Ballistic Missiles": Atlantic Council 2017.

Kendall, F. "State of Forces." Paper presented at the Air and Space Conference, 2021.

Kennedy, D. "How Iran Would Wage Cyber War against the United States". *The National Interest* (5 October 2019).

———. "Iran Is Building a Non-Nuclear Threat Faster Than Experts 'Would Have Ever Imagined'." By N. Bertrand. *Insider* (2015).

Keohane, R. . *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton Princeton University Press, 1984.

Keohane, R.O., and J.S. Nye. *Power and Interdependence.* 3 ed. Boston Longman 2012.

Kerns, A. "Unmanned Aircraft Capture and Control Via Gps Spoofing". *Journal of Field Robotics* 31, no. 4 (2014): 617-36.

Khan, A. . "The Extinction of Nation-State". *American University International Law Review* 7 (1992): 197- 234.

Khan, D. . *The Most in-Depth Hackers Guide: Hack Like a Pro! .* North Carolina: Lulu.com, 2015.

Khatami, M. "Statement by H.E. Mohammad Khatami President of the Islamic Republic of Iran before the 53rd Session of the United Nations General Assembly New York, September 21, 1998". Pars Times 1998.

Kindelberger, C. . "American Business Abroad." In *Globalisation, the New Economy and Regionalisation'*, edited by R. Sugden and J. R. Wilson: GaWC Research Bulletin, 1969. Reprint, 2001.

King, B. "Speech by New Zealand Secretary of Foreign Affairs and Trade", edited by New Zealand Government, 2018.

Kirby, P. "Is Russia Preparing to Invade Ukraine? And Other Questions", *BBC News Online*, 12 January 2021.

Klein, R.M., Lundqvist, S.. Pettersson, U. . "Baltics Left of Bang: The Role of Nato with Partners in Denial-Based Deterrence". *Strategic Forum* (November 2019).

Knighton, R. "Oral Evidence: Mod Annual Report and Accounts 2019-2." By House of Commons Defence Committee (8 December 2020).

Kochis, D. "Winds of Change in Berlin? A Road Map for U.S.–German Relations". *Heritage Foundation* (26 September 2021).

Korab-Karpowicz, W.J. . *Political Realism in International Relations - Stanford Encyclopaedia of Philosophy.* 2010.

Kornberg, J.F. "Comprehensive Engagement: New Frameworks for Sino-American Relations ". *The Journal of East Asian Affairs* 10, no. 1 (1996): 13-44.

Korolov, M. . "The List of Known Solarwinds Breach Victims Grows, as Do Attack Vectors": Data Centre Knowledge, 2021.

Kothari, C.R. *Research Methodology: Methods and Techniques.* New Delhi: New Age, 2004.

Kovacs, E. "$1.9 Million Paid out for Exploits at China's Tianfu Cup Hacking Contest". *Security Week* (19 October 2021).

Kramer, M. "The Myth of a No-Nato-Enlargement Pledge to Russia". *The Washington Quarterly* 32, no. 2 (2009): 39-61.

Krasner, S.D. . "Compromising Westphalia". *International Security* Winter (1996): 115-51.

———. *Sovereignty: Organised Hypocrisy* Princeton Princeton University Press, 1999.

Krauss, C. . "Oil Price Would Skyrocket If Iran Closed the Strait of Hormu", *New York Times*, 4 January 2012.

Krauthammer, C. "The Unipolar Moment". *Foreign Affairs* 70, no. 1 (1991): 23-33.

Krauthammer, C. . "The Unipolar Moment Revisited". *The National Interest* (2003): 5-18.

Krebs, B. . "Stolen Laptop Exposes Personal Data on 207,000 Reservists", In *Krebs on Security* 2010.

Krombholz, K. "Advanced Social Engineering Attacks". *Journal of Information Security and Applications* (July 2014).

Kshetri, N., and J. Voas. "Hacking Power Grids: A Current Problem". *Computer Fraud and Security* 50, no. 2 (2017): 91-95.

Kucinich, D. . "Obama Administration Must Account to Congress for Targeted Assassination", *The Guardian*, 16 November 2012.

Kuehl, D.T. . "From Cyberspace to Cyber Power: Defining the Problem." In *Cyberpower and National Security* edited by F.D. Kramer, S. Starr and L.K. Wentz, 34-56. Washington, D.C.: National Defense, 2009.

Kumar, C.R.S., Sanket, M. . "Current Trends in Cyber Security for Drones " Paper presented at the International Carnahan Conference on Security Technology (ICCST) 2021.

Lachow, I. . "The Upside and Downside of Swarming Drones". *Bulletin of the Atomic Scientists* 73, no. 2 (2017): 96-101.

Lague, D., Murray, M. "T-Day: The Battle for Taiwan ". *Reuters Investigates* (5 November 2021).

Lake, A. . "Confronting Backlash States". *Foreign Affairs* 73, no. 2 (March 1994): 45-55.

Lakshmanan, R. "New Study Links Seemingly Disparate Malware Attacks to Chinese Hackers", *The Hacker News* 5 October 2021.

Lambeth, B.S. *The Transformation of American Air Power* Ithica: Cornell University Press, 2000.

Lambeth, B.S. . *American Air Power* London: RAND, 2000.

———. *The Winning of Air Supremacy in Operation Desert Storm* Santa Monica: RAND, 1993.

Lantis, J.S. "Strategic Culture and National Security Policy". *International Studies Review* 4, no. 3 (2002): 87-113.

Lardy, N.R. "Issues in China's Wto Accession ". *Brooking Institute* (9 May 2001).

Larson, J.B. Letter 17 March 2020.

Lash, W.H. . "The Decline of the Nation State in International Trade and Investment". *International Trade and Investment* 18 (1996): 1011-25.

Lauterbach, T. "Constructivism, Strategic Culture, and the Iraq War". *ASPJ Africa & Francophonie* (2011): 61-91.

Lavrov, S. "Lavrov Predicts Historians May Coin New Term: The Primakov Doctrine." By Russian News Agency. *RNA Online* (28 October 2014).

Law, Robert Strauss Centre for International Security and. "Strait of Hormuz: Assessing the Threat to Oil Flows through the Strait": University of Texas, 2022.

Lawless, J. "Sanctions, Cyberattack among Possible Uk Moves on Russia", *AP News*, 13 March 2018.

Lawson, C. "Evaluating Inflight Ice Protection Methods for Application on Next Generation Aircraft". *Journal of Aerospace Engineering and Technology* 3, no. 3 (2019).

Lawson, P. *The East India Company: A History* London: Routledge, 1993.

Leal, D. "How Rishi Sunak Can Reset the Us-Uk Special Relationship", *The Hill*, 29 December 2022.

Lebovic, J.H. *Planning to Fail: The Us Wars in Vietnam, Iraq, and Afghanistan.* Oxford: Oxford University Press, 2019.

Lebow, R.N. "Thucydides the Constructivist". *The American Political Science Review* 95, no. 3 (2001): 547-60.

Lebow, R.N. . "Constructive Realism". *International Studies Review* 6 (2004): 346-48.

Lee, E.. Hsi-min, L. "Taiwan's Overall Defense Concept, Explained". *The Diplomat* (3 November 2010).

Lee, E.A. . "Cyber Physical Systems: Design Challenges", In *Technical Report No. UCB/EECS-2008-8 - Electrical Engineering and Computer Sciences* University of California at Berkeley, 2008.

Lee, G., and K. Ayhan. "Why Do We Need Non-State Actors in Public Diplomacy?: Theoretical Discussion of Relational, Networked and Collaborative Public Diplomacy". *Journal of International snd Area Studies* 22, no. 1 (2015): 57-77.

Lee, T.C. "Perspectives on Us Salesa of F-16 to Taiwan ". *The Journal of Contemporary China* 2, no. 1 (1993): 87-92.

Lee, Y. "Taiwan Leader Rejects China's 'One Country, Two Systems' Offer", *Reuters* 10 October 2019.

Lee, Y., Lague, D. . "T-Day: The Battle for Taiwan", *Reuters* 20 December 2021.

Lehto, E., and M. Stone. "Finland Orders 64 Lockheed F-35 Fighter Jets for $9.4 Bln", *Reuters* 10 December 2021.

Leiner, B.M., V.G. Cerf, D.D. Clark, R.E. Kahn, L. Kleinrock, D.C. Lynch, and S. Wolff. "A Brief History of the Internet", In *ACM SIGCOMM Computer Communication Review*, 22-31, 2009.

LePrestre, P.G. *Role Quests in the Post-Cold War Era* London: McGill-Queen's University Press, 1997.

Leung, J. . "Machiavelli and International Relations Theory". *Glendon Journal of International Studies* 1 (2000): 1-11.

Levie, H.S. . "History of the Law of War on Land": International Review of the Red Cross, 2000.

Levinson, S. . *Mathematical Models for Speech Technology* Illinois: Wiley, 2005.

Lewis, J. "Cyber War and Ukraine": Center for Strategic and International Studies, 2022.

———. "Defence Spending Continues to Decline", edited by UK Parliament: HM Government 2019.

Lewis, J.A. "Cyber-Attacks Explained". *Centre for Strategic and International Studies* (15 June 2007).

Lewis, M. W. . "The Law of Aerial Bombardment in the 1991 Gulf War'". *The American Journal of International Law* 97, no. 3: 481-509.

Lewis, P., and B. Unal. "Cyberattacks on Missile Systems". *Chatham House* (2 July 2019).

Leyden, J. "Mystery Virus Attack Blows Qatari Gas Giant Rasgas Offline". *The Register* (30 August 2012).

Li-hau, C. "5,000 Chinese Spies in Taiwan", *Taipei Times*, 13 March 2017.

Libicki, M.C. . "Cyberspace Is Not a Warfighting Domain". *ISJLP* 82 (2013): 321-36.

———. "Why Cyber War Will Not and Should Not Have It Grand Strategist". *Strategic Studies Quarterly* 8, no. 1 (22-39 2014).

Lieberthal, K.G. . "The American Pivot to Asia ". *Brooking Institute* (21 December 2011).

Lillemose, A., and Krygerm M. "The (Re)Invention of Cyberspace". *The Nordic Art Review* (24 Augus 2015).

Lilly, B., and J. Chersvitch. "The Past, Present and Future of Russia's Cyber Strategy and Forces", In *12th International Conference on Cyber Conflict* 128-65. Tallinn NATO CCDCOE, 2020.

Lincoln, Y.S. *Handbook of Qualitative Research.* California: Sage, 1994.

Linde, R.R. . "Operating System Penetration", In *National Computer Conference and Exposition*, 1975.

Lindell, J. . "Clausewitz: War, Peace and Politics". *E-International* (26 November 2009).

Lindsay, J.R. . "Stuxnet and the Limits of Cyber Warfare". *Security Studies* 22, no. 3 (2013): 365-404.

Lippmann, W. *Public Opinion and Foreign Policy in the United States.* London: Allen and Unwin, 1952.

Lissitzyn, O.J. . "The Treatment of Aerial Intruders in Recent Practice and International Law". *The American Journal of International Law* 47, no. 4 (1953): 559-89.

Litsas, S.N. "Russian in the Eastern Mediterranean: Intervention, Deterrence, Containment". *Digest of Middle East Studies* 26, no. 1 (2017): 56-73.

Little, R. "The Eclectic and Pragmatic Heritage of Ir Theory." In *Perspectives on World Politics* edited by R. Little and M. Smith, 1-14. London: Routledge, 2006.

Little, R. . "Neorealism and the English School: A Methodological, Ontological and Theoretical Reassessment". *European Journal of International Relations* 1, no. 1 (1995): 9-34.

Lloyd, T. *Empire: A History of the British Empire.* London: Hambledon, 2001.

Lobell, S.E. . "Structural Realism / Offensive and Defensive Realism." In *Oxford Research Encyclopaedia of International Studies* Oxford: Oxford University Press, 2010.

Lockheed-Martin. "Autonomic Logistics Information System (Alis) ", 2018.

———. "The Global F-35 Enterprise ", 2021.

———. "Meet F-16v: The Most Technologically Advanced 4th Generation Fighter in the World." https://www.lockheedmartin.com/en-us/news/features/2016/meet-the-f-16v--the-most-technologically-advanced-4th-generation.html#:~:text=The%20F%2D16V%20configuration%20includes,Generation%20multi%2Drole%20fighter%20aircraft.

———. "The Most Advanced Fighter Jet in the World ", 2021.

LockheedMartin. "About the F-35: The Multi-Variant, Multirole 5th Generation Fighter", 2020.

Long, A., and B.R. Green. "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy". *Journal of Strategic Studies* 38, no. 1 (2015): 38-73.

Long, D., and P. Wilson. *Thinkers of the Twenty Years' Crisis: Inter-War Idealism Reassessed* Oxford Oxford University Press, 1995.

Lord, W. "Testimony for the Senate Foreign Relations Committee, Asia and Pacific Subcommittee by Winston Lord, Assistant Secretary for East Asian and Pacific Affairs, Department of State", edited by US Department of State. Archive 1995.

Lowther, A.B. . "Air Diplomacy: Protecting American National Interests". *Strategic Studies Quarterly* 4, no. 3 (2010): 2-14.

Lucas, E., Hodges, B., Schmiedl, C. . "Close to the Wind: What Russia Wants". *Center for European Policy Analysis* (9 September 2021).

Ly, B. and Ly, R. "Cybersecurity in Unmanned Aerial Vehicles (Uavs)". *Journal of Cyber Security Technology* (November 2020): 1-18.

Lydiate, D. "Swimming with Our Eyes Open". *ITNOW* (June 2020): 16-17.

Lye, H. "Uk Mod Civilian Head Cases Doubt on 138 F-35 Fleet Number". *Airforce Technology* (9 February 2021).

Lynch, A.C. "The Evolution of Russian Foreign Policy in the 1990s". *The Journal of Communist Studies and Transition Politics* 18, no. 1 (2002): 161-82.

Lynch, J. "The Myth of American Military Dominance". *War on the Rocks* (15 August 2019 2019).

Lyngaas, S. "Revisiting the Navy's Blueprint for Cyber Operations". *FCW* (18 March 2015).

Lynn, W. "Defencing a New Domain". *Foreign Affairs* (September 2010).

Lyon, D. . "From 'Post-Industrialism' to 'Information Society: A New Social Transformation? ". *Sociology* 20, no. 4 (1986): 577-88.

Ma, A. "How the Strait of Hormuz, a Narrow Stretch of Water Where Ships Carry $1.2 Billion of Oil Every Day, Is at the Heart of Spiraling Tensions with Iran". *Business Insider* (13 January 2020).

Macak, K. . "This Is Cyber: 1+3 Challenges for the Application of International Law in Cyberspace". *Working Paper Series, Exeter Centre for International Law* (2019).

MacAskill, A., Saul, J. . "Britain Begins Escorting All Uk Vessels through Hormuz Strait", *Reuters* 25 July 2019.

MacAskill, E. "Obama Appeals to Iran to Return Downed Us Spy Drone", *The Guarian* 12 December 2011.

MacColl, J., and S. Dawda. "Us Water Plant Suffers Cyber-Attack through the Front Door". *RUSI Commentary* (10 February 2021).

Machain, C.M. "Exporting Influence: U.S. Military Training as Soft Power". *Journal of Conflict Resolution* 65, no. 2-3 (16 September 2020).

Machi, V. "How the F-35 Swept Europe, and the Competition It Could Soon Face", *Defense News* 4 September 2022.

———. "State Department Approves $8.4 Billion F-35 Sale to Germany", *Defense News*, 22 July 2022.

Machiavelli, N. . *The Prince* London: Penguin, 1513.

Macola, G. . "The Five Worst Cyber-Attacks against the Power Industry since 2014", *Power Technology*, 2 April 2020.

Magee, C. "Awaiting the Cyber 9/11." USMC University, 2012.

Maglaras, G.B., and S.M. Furnell. "Insider Threat Prediction Tool: Evaluating the Probability of It Misuse". *Computers and Security* 21, no. 1 (2001): 62-73.

Mahnken, T.G. "United States Strategic Culture". Advanced Systems and Concepts Office: Defense Threat Reduction Agency, 2006.

Majumdar, D. . "Usmc Finds Workaround for Cyber-Vulnerability of F-35 Logistics System", *Flight Global*, 21 November 2012.

Malaska, P. . "Knowledge and Information in Futurology". *Foresight: The Journal of Future Studies* 2, no. 2 (2000): 237-44.

Mandiant. "Apt1 Threat Intelligence Report ", 2013.

Mansoor, P.R. . "Hybrid War in History." In *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* edited by M. Williamson and P.R. Mansoor. Cambridge Cambridge University Press, 2012.

Mapscapping.com. "What Is Topography? ." https://mapscaping.com/blogs/news/what-is-topography.

Marcus, J. . "Could an Ancient Greek Have Predicted the Us-China Conflict?", *BBC News Online*, 25 March 2019.

Marin, L. . "Is Europe Turning into a 'Technological Fortress'? Innovation and Technology for the Management of Eu's External Borders: Reflections on Frontex and Eurosur." In *Regulating Technological Innovation* edited by M. A. Heldeweg and E. Kica, 131-51. London: Palgrave McMillan.

Markoff, J. . "Before the Gunfire, Cyberattacks", *The New York Times*, 12 August 2008.

Marten, K. "Nato Enlargement: Evaluating Its Consequences in Russia". *International Politics* 57 (2020): 401-26.

Martinich, A.P. . *Hobbes.* London: Routledge, 2005.

Mason, R.A. . "The Air War in the Gulf". *Survival* 33, no. 3 (1991): 211-29.

Masood, T., and P. Sonntag. "Industry 4.0: Adoption Challenges and Benefits for Smes". *Computers in Industry* 121 (2929).

Massberg, M., J. Warren, and N.L. Beebe. "The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits", In *48th International Conference on System Sciences*, 3518-26. Hawaii 2015.

Masters, J. . "Ukraine: Conflict at the Crossroads of Europe and Russia". *Council on Foreign Relations* (5 February 2020).

Matsumoto, H. . "The First Taiwan Strait Crisis and China's" Border" Dispute around Taiwan ". *Eurasia Border Review* 3 (2012): 75-91.

Matteo, C. . "How and to What Extent Do the Baltic States Feel Geopolitically Threatened". *Journal of Diplomacy and International Relations* 16, no. 2 (2015): 77-92.

Mattern, J. . "Why Soft Power Isn't So Soft: Representational Force and the Sociolinguistic Construction of Attraction in World Politics". *Millennium* 33 (2005): 583–612.

Mattern, J.B. "Power in Realist-Constructivist Research". *International Studies Review* 6, no. 2 (2004): 343-46.

Mattis, J.N. . "Military High Tech Leads to Big Graft." By S. Beauchamp (29 November 2014).

Mattis, P. "A Guide to Chinese Intelligence Operations ". *War on the Rocks* (18 August 2015).

May, A. . "The Commonwealth and Britain's Turn to Europe: 1945-83". *", The Round Table: The Commonwealth Journal of International Affairs* 1, no. 102 (2013): 29-30.

May, T. "Pm Commons Statement on Salisbury Incident", edited by Gov.UK, 2018.

May, T. . "The Government's Negotiating Objectives for Existing the Eu: Pm Speech", edited by Cabinet Office. Gov.UK, 2017.

———. "Pm Speech at Munich Security Conference", edited by Cabinet Office. Gov.UK, 2018.

McClory, J. "The New Persuaders: An International Ranking of Soft Power": Instiute for Government 2010.

McClure, S. "Iranian Hackers Planning Attack on U.S. Energy Firms and Universities, Fbi Warns." By Staff Writer. *Daily Mail* (13 December 2014).

McDermott, J.P. . "Attack Net Penetration Testing", In *Proceedings of the Workshop on New Security Paradigms*, 2001.

McInnis, J. K. and Starling, C. G. . "The Case for a Comprehensive Approach 2.0: How Nato Can Combat Chinese and Russian Polical Warfare", edited by Scrowcroft Centre for Strategy and Security. Washington D.C: Atlantic Council 2020.

McKew, M.K. "The Gerasimov Doctrine". *Politico* (October 2017).

McKey, M.K. . "The Gerasimov Doctrine", *Politico*, October 2017.

McKinney, B. . "Using Automation and Robotics in Advanced Aircraft Production": Northrop Grumman, 2022.

McMillan, R. "Woman Helped Sell Fake Chips to Us Military", *PC World News*, 23 November 2010.

McNamara, R.S., Blight, J.G. *Wilson's Ghost: Reducing the Risk of Conlfict, Killing and Catastrophe in the 21st Century* New York Public Affairs, 2001.

McNeill, P., and S. Chapman. *Research Methods.* London: Routledge, 2005.

Mdzinarishvill, D. . "Why Putin Took Crimea: The Gambler in the Kremlin". *Foreign Affairs* (May/June 2016).

Mearsheimer, J.J. *The Tragedy of Great Power Politics* New York: Norton Publishing Company, 2001.

Mearsheimer, J.J. . *Structural Realism’ in International Relations Theories: Discipline and Diversity* Oxford: Oxford University Press, 2007.

Media, Small. "Iranian Internet Infrastructure and Policy Report: Special Edition - the Rouhani Review (2013–15)", 2015.

Menn, J. . "Russian Researchers Expose Breakthrough Us Spying Program", *Reuters*, 16 February 2015.

Merkel, A. "Merkel Pledges Nato Will Defence Baltic Member States." By Reuters Staff. *Reuters* (18 August 2014).

Mesterhazy, A. "Burden Sharing: New Commitments in a New Era", edited by NATO Parliamentary Assembly Defence and Security Committee, 2018.

Meuller, K. . "The Essence of Coercive Air Power: A Primer for Military Strategists". *Air Power Review* 4, no. 3 (2001): 45-56.

MI5. "Intelligence and Security Committee of Parliament: Annual Report, 2016-2017", edited by HouseofCommons, 2017.

Miani, R.S., G. Vasconcelos, J. Souza, and V. Guizillini. "The Impact of Dos Attacks on the A.R.Drone 2.0", In *XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR)* 127-32. Brazil, 2016.

Microsoft. "New “Prestige” Ransomware Impacts Organizations in Ukraine and Poland": Microsoft, 2022.

———. "Threat Actor Dev-0322 Exploiting Zoho Manageengine Adselfservice Plus". Microsoft.Com, 2021.

Miller, B. . "The Concept of Security: Should It Be Redefined?". *Journal of Strategic Studies* 24, no. 2 (2001): 14-42.

Miller, B., and D. Rowe. "A Survey of Scada and Critical Infrastructure Incidents", In *1st Annual conference on Research in Information Technology*, 51-56, 2012.

Miller, M. "Russian Invasion of Ukraine Could Redefine Cyber Warfare", *Politico* 28 January 2022 2022.

Milot-Poulin, J., Sarfati, R., Paquin, J. "The American Strategic Pivot in the Indo-Pacific ". *Policy* 15 (2021).

Mirow, W. *Strategic Culture, Securitisation and the Use of Force: Post-9/11 Security Practices of Liberal Democracies.* London: Routledge, 2016.

Mitchell, W. *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military.* Alabama: University of Alabama Press, 1925.

Mizokami, K. . "The F-16v, the Newest Version of the Iconic Fighter, Takes Flight". *Popular Mechanics* (2015).

Molloy, S. . "Truth, Power, Theory: Hans Morgenthau's Formulation of Realism". *Democracy and Statecraft* 15 (2008): 1-34.

Monaghan, A. "The 'War' in Russia's 'Hybrid Warfare'". *Parameters* 45, no. 4 (2015): 65-74.

Monaghan, S. "The Joint Expeditionary Force: Global Britain in Northern Europe?". *Center for Strategic and International Studies (CSIS)* (25 March 2022).

Montgomery, B.L. . "The Role of Science in Warfare of the Future". *Engineering and Science* 18, no. 3 (1954): 20-28.

Moore, G.E. . "Cramming More Components onto Integrated Circuits". *Electronics* 38, no. 8 (19 April 1965).

Morgan, P.M., and T.V. Paul. "Deterrence among Great Powers in an Era of Globalisation." In *Complex Deterrence: Strategy in the Global Age* edited by T.V. Paul, 259-319. Chicago: University of Chicago Press, 2009.

Morgenthau, H.J. "The Hopelessness of Victory". *Foreign Affairs* 32, no. 2 (1954): 221-29.

———. *Politics among Nations: The Struggle for Power and Peace* New York: Knopf, 1948.

Morris, J. "How Great Is Britain? Power, Responsibility and Britain's Future Global Role". *The British Journal of Politics and International Relations* 13, no. 3 (2011): 326-47.

Moschovitis, C. . "Why So Cyber Security Programmes Fail?". *Cyber Security* 2, no. 4 (2019): 303-09.

Moutray, R.E., and A.M. Ponsford. "Integrated Maritime Surveillance: Protecting National Sovereignty', " In *International Conference on Rada*, 2003.

Mueller, K.P. . *Precision and Purpose: Airpower in the Libyan Civil War* Santa Monica: RAND, 2015.

Mujumdar, D. "New Report Details Why a War between China and America Would Be Catastrophic". *The National Interest* (1 August 2016).

Murray, R.W. "Intervention in the Emerging Multipolar System: Why R2p Will Miss the Unipolar Moment". *Journal of Intervention and Statebuilding* 6, no. 4 (2013): 387-406.

Muzyka, K. . "Russia Goes to War: Exercises, Signalling, War Scare and Military Confrontations". *Centre for Strategic and International Studies* (28 July 2021).

Myers, L. "Albright, Ian Minister Meet", *AP*, 22 September 1998.

Nadimi, F. "The Irgc and the Persian Gulf Region in a Period of Contested Deterrence". *The Middle East Institute* (November 2021).

Naegele, T. "The Best Fighter in the World", *Air Force Magazine*, 26 March 2021.

Nakashima, E. "Cyber-Intruder Sparks Massive Federal Response and Debate over Dealing with Threats", *Washington Post*, 9 December 2011.

———. "Defense Official Discloses Cyberattack", *Washington Post*, 24 August 2010.

Nakashima, E. . "Russia Military Was Behind ‘Notpeya’ Cyberattack in Ukraine, Cia Concludes", *Washington Post*, 12 January 2018.

Nakasone, P.M. "Cybercom Sent a ‘Hunt Forward’ Team to Help Ukraine Harden Systems." By L. Johnson. *MeriTalk* (5 April 2022).

———. "Statement of General Paul M. Nakasone, Commander United States Cyber Command, before the Senate Committee on Armed Services", edited by Senate Committee on Armed Services, 2019.

Nations, United. "1944-1945: Dumbarton Oaks and Yalta ", edited by UN Secretariat, 2020.

———. "United Nations Convention on the Law of the Sea (Unclos)", 1982.

NATO. "Baltic Air Policing ", edited by NATO Newsroom, 2020.

———. "Boosting Nato’s Presence in the East and Southeast", edited by NATO Newsroom, 2022.

———. "Cyber Defence ", 2019.

———. "Hungary to Lead Nato’s Baltic Air Policing, Joined by Uk and Spain ", 2019.

———. "Joint Intelligence, Surveillance and Reconnaissance", edited by NATO Newsroom, 2018.

———. "Member Countries", 2020.

———. "Nato Cyber Defence - Nato Fact Sheet", 2016.

———. "Nato Strategic Concept", 2022.

———. "New Nato Force Model ", 2022.

———. "The Power of Nato's Military", edited by NATO Newsroom, 2022.

———. "Russian Fighter Jet Violated Nato Airspace over Bornholm Island’", edited by NATO Newsroom, 2020.

———. "Strategic Concept: For the Defence and Security of the Members of Nato", 2010.

———. "Warsaw Summit Communiqué", edited by NATO Press Release, 2016.

Naughton, J. . "The Evolution of the Internet: From Military Experiment to General Purpose Technology’". *Journal of Cyber Policy* 1, no. 1 (2016): 5-28.

Newman, L. "Inside the Unnerving Supply Chain Attack That Corrupted Ccleaner", *Wired* 17 April 2018.

Newton, R.Y. . "Air Force Leaders Call People Greatest Asset." By C. N. McLuney. *Department of Defence News* (17 September 2010).

Nicas, J., and Z. Wichter. "A Worry for Some Pilots: Their Hands-on Flying Skills Are Lacking’", *The New York Times*, 14 March 2019.

Nicholas, S. "Gen. Ellen Pawlikowski: Cyber Resiliency Steering Group Unveils Air Force Cyber Campaign Plan", *Executive Gov* 23 September 2016.

Nicholls, D. . "Has the Royal Navy Got Enough Ships?", *The Telegraph*, 24 January 2020.

Nicholson, A., S. Webber, S. Dyer, T. Patel, and H. Janicke. "Scada Security in the Light of Cyber-Warfare". *Computers and Security* 31, no. 4 (2012): 418-36.

Nightengale, W.S. . "The Changing Face of War: Into the Fourth Generation". *Marine Corps Gazette* (October 1989): 22-26.

NIST. "Cyber Supply Chain Risk Management": National Institute of Standards and Technology 2020.

———. "Framework for Improving Critical Infrastructure Cybersecurity": National Institute of Standards and Technology 2018.

———. "Key Practices in Cyber Supply Chain Risk Management": National Institute of Standards and Technology 2020.

Nobles, C. *Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications.* Pennsylvania: IGI Global 2019.

Nofi, A.A. . *Recent Trends in Thinking About Warfare* Alexandria: CAN Corp, 2006.

Nolin, P. C. . "Unmanned Aerial Vehicles: Opportunities and Challenges for the Alliance’". *NATO International Secretariat Special Report* (2012).

Norman, A. . "Can the Us Military’s New Jet Fighter Be Hacked?" By D. Martin. *60 Minutes* (2014).

Northcutt, S. . "Logic Bombs, Trojan Horses and Trap Doors". *Sans Technology Institute* (June 2018).

Norton. "Malware – What Is a Trojan? ", 2020.

Norton, N. "The U.S. Navy’s Evolving Cyber/Cybersecurity Story". *The Cyber Defense Review* 1, no. 1 (Spring 2916): 21-26.

NSA, CISA, FBI and NCSC. "Russian Gru Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments", edited by Cybersecurity Advisory Note, 2021.

Nunes, M. . "Virtual Topographies: Smooth and Striated Cyberspace." In *Cyberspace Textuality: Computer Technology and Literary Theory* edited by M. Ryan, 61-77. Indiana: Bloomington, 1999.

Nurse, J. R., O. Buckley, P.A. Legg, M. Goldsmith, S. Creese, G.R. Wright, and M. Whitty. "Understanding Insider Threat: A Framework for Characterising Attacks". *Security and Privacy Workshops* (May 2014): 214-28.

Nye, J. S. "Public Diplomacy and Soft Power". *The Annals of the American Academy of Political and Social Science* 616, no. 1 (2008): 94-109.

———. *Soft Power: The Means to Success in World Politics* New York: Perseus Books Group, 2004.

Nye, J.S. "Get Smart: Combining Hard and Soft Power". *Foreign Affairs* 88, no. 4 (July 2009): 160-63.

Nye, J.S. . "Combining Hard and Soft Power". *Foreign Affairs* 68, no. 4 (2009): 160-63.

———. *Cyber Power.* Cambridge, MA: Harvard University Press, 2010.

Nye, J.S., and W.A. Owens. "America’s Information Edge". *Foreign Affairs* 75, no. 2 (March 1996): 20-23.

O'Hanlon, M. "China, the Grey Zone, and Contingency Planning at the Department of Defence and Beyond". *Brooking Institute* (September 2019).

O'Neill, P. . "Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion". *MIT Technilogy Review* (10 May 2022).

O'Toole, R. . "Hearing to Receive Testimony on Defense Aquisition Prograems and Aquisition Reform ", edited by United States Senate Committee on Armed Services, 2021.

O'Connell, K. M. . "'Uncle Wiggle Wings': Children, Chocolates and the Berlin Airlift". *Food and Foodways* 25, no. 2 (2017): 1420159.

O'Raw, J., and D. Laverty. "Restricting Data Flows to Secure against Remote Attacks", In *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* 1-4, 2020.

Oakley, J.G. . *Waging Cyber War: Technical Challenges and Operational Constraints.* New York: Apress, 2019.

Oam, S.W. . "Nuclear Deterrence Theory-a Threat to Inflict Terror". *Flinders Law Journal* 15 (2013): 257-72.

Obama, B. "Obama's 'Brexit' Plea." By K. Calamur (22 April 2016).

Obama, B. . "Remarks by President Obama and Prime Minister Al-Maliki of Iraq in a Joint Press Conference", edited by Office of the Press Secretary: The White House, 2011.

Olejnik, L. "Global Consequences of Escalating Us – Russia Cyber Conflict". *Council on Foreign Relations* (2 April 2019).

Olejnik, L. . "Target Confirming an Offensive Cyber Operation". *Security Privacy and Tech Inquirie* (1 March 2019).

Olive, M.L., R.T. Oishi, and S. Arentz. "Commercial Aircraft Information Security - an Overview of Arnc Report 811", In *25th Digital Avionics Systems Conference*, 1-12, 2006.

Olsen, J.A. . *Strategic Air Power in Desert Storm* London: Routledge, 2003.

Olson, J. . "The Effect of Civilian Casualties on Usaf Bombing Policy in Vietnam". *Air Power History* 46, no. 44= (1999).

Online, The Week. "The Commonwealth: Why It Struggles to Remain Relevant", *The Week*, 1 August 2014.

Onslow, S. . "The Commonwealth and the Cold War, Neutralisation and Non-Alignment". *The International History Review* 37 (2015): 1059-82.

Onuf, N.G. . *World of Our Making.* South Carolina: University of South Carolina Press, 1989.

Oppermann, K., Beasley, R., Kaarbo, J. . "British Foreign Policy after Brexit: Losing Europe and Finding a Role". *International Relations* July (2019): 1-24.

Orenstien, M. "Russia's Use of Cyberattacks Lessons from the Second Ukraine War". *Foreign Policy Research Institute* (7 June 2022).

Orgeron, B. "F-15ex and F-35a: The Future of American Air Superiority". *War on the Rocks* (30 May 2019).

Osborn, K. "Even with Upgrades, Chinese J-15 Are No Match for American Fighters". *The National Interest* (31 December 2021).

———. "The F-35's Cyber Reliance Makes It Powerful—but Also Vulnerable to Attack". *National Interest* (21 December 2021).

———. "Japan Launches F-35b from Destroyer - to Neutralize China's Fleet of J-20 & J-31 Fighter Jets", *Warrior Maven* 29 July 2022.

———. "U.S. Air Force: F-16s and Other Critical Weapons May Be Vulnerable to Cyber Attack". *The National Interest* (23 September 2016).

———. "The U.S. Army's Future: All About Robots?". *National Interest* (16 June 2021).

———. "Why the F-15 Eagle and F/a-18 Super Hornet Are Still Useful". *The National Interest* (24 January 2022).

Osborne, C. "Air Force: An F-16 Could Be Vulnerable to Cyber Attack", *Defence Systems* 18 October 2016.

Ottis, R. "Analysis of the 2007 Cyber-Attacks against Estonia from the Information Warfare Perspective", In *7th European Conference on Information Warfare* 151-68, 2004.

Ovendale, R. . *Anglo-American Relations in the Twentieth Century* Basingstoke MacMillan, 1998.

Overholt, W.H. "Hong Kong: The Rise and Fall of 'One Country, Two Systems'". *Ash Center for Domocratic Governance , University of Harvard* (December 2019).

Overy, R.J. . "Air Power and the Origins of Deterrence Theory before 1939". *The Journal of Strategic Studies* 15, no. 1 (1992): 73-101.

Oxford-Dictionary. "Definition of Cyber ". In *Oxford Dictionary* Oxford Oxford University Press, 2015.

P., Suciu. "U.S. Air Force Sends F-22s to the Uae after Surge in Houthi Attacks". *The National Interest* (16 February 2022).

Page, L. . "Israeli Sky-Hack Switched Off Syrian Radars Countrywide’", *The Register*, 22 November 2007.

Pamment, J. *British Public Diplomacy and Soft Power: Diplomatic Influence and the Digital Revolution.* London: Springer, 2016.

Panda, A. "Obama: Senkakus Covered under Us-Japan Security Treaty". *The Diplomat* (24 April 2014).

Panda, A. . "North Korea, Us ‘Left of Launch’ Cyber Capabilities and Deterrence", *The Diplomat*, 6 December 2018.

Panetta, L.E. . "Panetta Warns of Dire Threat of Cyberattack on Us." By E. Bumiller and T. Shanker (11 October 2012).

Pape, R. "The True Worth of Air Power". *Foreign Affairs* 83, no. 2 (2004): 116-30.

Pape, R.A. *Bombing to Win: Air Power and Coercion in War* Ithica: Cornell University Press, 1996.

Pape, R.A. . "The True Worth of Air Power". *Foreign Affairs* 83 (2004).

Pardew, J.W. . "The Iraqi Army’s Defeat in Kuwait". *US Defence Technical Information Centre* 17 (1991).

ParisConvention. "Convention for the Regulation of Aerial Navigation". *The American Journal of International Law* 17, no. 4 (1923): 195-212.

Parry, C. "The United Kingdom’s Future Carriers: What Are the Good For?". *RUSI Journal* 157, no. 6 (21 May 2012): 4-9.

Pasandideh, S. . "Do China’s New Islands Allow It to Militarily Dominate the South China Sea?". *Asian Security* 17, no. 1 (2020): 1-24.

Paul, T.V. . *Complex Deterrence: Strategy in the Global Age.* Chicago University of Chicago Press, 2009.

Paulhus, D.L., and K.M. Williams. "The Dark Triad of Personality: Narcissism, Machiavellism and Psychopathy". *Journal of Research in Personality* 36 (2000): 556-63.

Pauli, D. . "Your Hard Drives Were Riddled with Nsa Spyware for Years’". *The Register* (17 February 2015).

Payne, K. . *Deterrence in the Second Nuclear Age* Lexington Kentucky University Press, 1996.

Pederson, S. *The Guardians: The League of Nations and the Crisis of Empire.* Oxford: Oxford University Press 2015.

Pend, L. "New Zealand’s Subtly Shifting Foreign Policy". *The Diplomat* (January 2022).

Perju, V. . "Precision Guided Bombs: Analysis". *Revisita Militara* 2, no. 22 (2019): 111-19.

Perkins, W.A. . "Enabling Maritime Isr through the ‘Family of Systems’". *The Journal of the Joint Air Power Competence Centre* July (2017): 15-18.

Perrotto, T. . "China Key Suspect in Us Satellite Hacks." By J. Wolf (28 October 2011).

Peters, J. A., and D. M. Lodge. "Littoral Zone." In *Encyclopaedia of Waters* edited by G. E. Likens. New York: Elsevier, 2009.

PewResearchCentre. "Views on the Us and American Foreign Policy", In *Global Attitudes and Trends*, 2012.

Pidgeon, N.R. "Risk Perception within Risk – Analysis, Perception and Management": Royal Society Study Group, 1992.

Pierce, D. "America in the Post War Period". *Inquiries* 1, no. 10 (2009,).

Pietrucha, M., and J. Renken. "Air Power May Not Win Wars, but It Sure Doesn't Lose Them". *War on the Rocks* (19 August 2015).

Plaw, A., M. S. Fricker, and C. R. Colon. *The Drone Debate: A Primer on the Us Use of Unmanned Aircraft Outside Conventional Battlefields* London: Rowman and Littlefield, 2015.

Ploeger, D.C., R.B. Chapman, D.G. Peshkin, and D.J. Speidel. "Airport Cooperative Research Program (Acrp) Report 138: Aviation Infrastructure ". Washington D. C.: Transportation Research Board, 2015.

Pollpeter, K. . "Testimony before the Us China Economic and Security Review Commission: Hearing on China’s Advanced Weapons", edited by Economic and Security Review Commission, 2017.

Pollpeter, K., M.S. Chase, and E. Heginbotham. "The Creation of the Pla Strategic Support Force and Its Implications for Chinese Military Space Operations". *RAND* (2017).

Ponemon-Institute. "Study on the Cyber Resilient Organisation ", 2019.

Porter, P. *The Global Village Myth: Distance, War and the Limits of Power* Georgetown: Georgetown University Press, 2015.

Porter, P. . "Why Britain Doesn't Do Grand Strategy". *The RUSI Journal* 155, no. 4 (2010): 6-12.

Posaner, J. "‘Hand-in-Hand’: Finland, Sweden Pledge to Join Nato Together", 29 October 2022.

Posey, C. . "Air War in the Falklands". *Air and Space Smithsonian* 17, no. 3 (2002): 70-79.

Powell, R. . "Nuclear Deterrence Theory, Nuclear Proliferation, and National Missile Defense". *International Security* 27, no. 4 (2003): 86-118.

Prentice, B., and P. Mee. "Aviation Industry May Be Vulnerable to Cyberattack through Its Global Supply Chain", *Forbes*, 11 April 2018.

Press, The Associated. "Berlin Airlift: Germans Look Back and Forward", *NBC News* 2008.

Pringle, R.W. "The Heritage and Future of the Russian Intelligence Community". *International Journal of Intelligence and Counter Intelligence* 11, no. 2 (2008): 175-84.

Pryor, C.D. "Taiwan's Cybersecurity Landscape and Opportunities for Regional Partnership". *Center for Strategic and International Studies (CSIS)* (2018).

Quinian, S. . "Jam. Bomb. Hack? New Us Cyber Capabilities and the Suppression of Enemy Air Defences". *Georgetown Security Studies Review* (7 April 2014).

Quinn, J. "What Is the Status of the British F035 Fleet?" By G. Allison. *UK Defence Journal* (27 July 2021).

R.F., Al Rodhanm. "U.S. Space Policy and Strategic Culture". *Journal of Interational Affairs* (16 April 2018).

Raab, D. "Global Britain Is Leading the World as a Force for Good", *The Telegraph* 21 September 2019.

Raab, D. . "Uk Condemns Russia's Gru over Georgia Cyber-Attacks'", edited by Gov.UK - Press Release, 2020.

Rajagopalan, R.P. "Electronic and Cyber Warfare in Outer Space": United Nations Institute for Disarmament Research, 2019.

Ranadive, V. . "Hypoconnectivity: The Future Is Now'", *Forbes*, 19 February 2013.

Rashid, F.Y. . "Cyber-Attackers Breach Scada Network, Destroy Pump at Water Utility'", *eweek*, 18 November 2011.

Ray, J.L. "The Abolition of Slavery and the End of International War". *International Organisation* 43 (1989): 405-39.

Ray, J.L. . "Does Interstate War Have a Future? ". *Conflict Management and Peace Science* 19, no. 1 (2003): 53-80.

Redman, L.V, and A.V.H. Mory. *The Romance of Research* Philadelphia: The Williams & Wilkins Company, 1933.

Redondo, A., A. Torres-Barran, D. R. Insua, and J. Domingo. "Assessing Supply Chain Cyber Risks". *2019* arXivLabs Cornell University (27 November 2019).

Rees, N. . "Raf's Quick Reaction Alert Reveale", *News Story*, 20 September 2012.

Rees, W. Aldrich, R.J. "Contending Cultures of Counterterrorism: Transatlantic Divergence or Convergence". *International Affairs* 81, no. 5 (2005): 905-23.

Reim, G. . "First Lockheed Martin F-35s Loaded with Odin Hardware'", *Flight Global*, 9 October 2020.

Rein, C. . "Nato Air Deployments to the Baltics as Strategic Messaging." In *The Challenge to Nato: Global Security and the Atlantic Alliance* edited by M.O. David Slobodchikoff, G.D., Stewart, B. , 75-96. Washington D.C.: Libary of Congress, 2021.

Renner, R.A. . "America’s Asymmetric Advantage: The Utility of Airpower in the New Strategic Environment". *Defence Studies* 4, no. 1 (2004): 87-113.

Republique-Française. "Defence and National Security Review: Strategic Review ". France, 2017.

Reus-Smit, C. "Constructivism and the English School." In *Theorising International Society* edited by C. Navari. London: Palgrave Macmillan, 2009.

Reynolds, D. . "A ‘Special Relationship’? America, Britain and the International Order since the Second World War". *International Affairs* 62, no. 1 (1986): 1-20.

Ricketts, P. "Brexit Makes Britain ‘Less Useful to the Us’." By C. Gallardo (26 October 2020).

Ricks, T.E. *Fiasco: The American Military Adventure in Iraq.* New York: Penguin Press, 2006.

Rid, T. . "Cyber War Will Not Take Place". *Journal of Strategic Studies* 35, no. 1 (2012): 5-32.

Riftkin, J. . "Leading the Way to the Third Industrial Revolution". *European Energy Review* 1 (2008): 1-36.

Robinson, E.W. . "What Thucydides Teaches Us About War, Politics and the Human Condition", *War on the Rocks*, 9 August 2017.

Robinson, M. . "The Scada Threat Landscape", In *1st International Symposium for ICS & SCADA Cyber Security Re*, 40-41, 2013.

Roblin, S. "Israel's F-35 Stealth Fighters Can Strike Iran at Any Moment". *National Interest* (9 November 2019).

———. "Who Deserves the Blame for the F-35's Many Computer Problems". *National Interest* (26 March 2020).

———. "Why China Has Went All-in on Chinese A2/Ad". *The National Interest* (10 January 2021).

Roblin, S. . "Can China’s Chengdu J-20 Stealth Fighter Win against America’s F-35 or F-22", *National Interest*, 14 September 2019.

———. "Some Sixth-Generation Stealth Fighters May Never Get Off the Ground", *National Interest*, 20 April 2021.

———. "Us Aircraft Carriers in South China Sea Make Needed Show of Force against Beijing", *NBC News*, 8 July 2020.

Rodofile, N.R., K. Radke, and E. Foo. "Extending the Cyber-Attack Landscape for Scada-Based Critical Infrastructure". *International Journal of Critical Infrastructure Protection* 25 (June 2019): 14-35.

Roosevelt, F. . "Four Freedoms Speech, State of the Union Address". Franklin D. Roosevelt Presidential Library 1941.

Roosevelt, F.D. . "Four Freedoms Speech". *American Rhetoric: Top 100 Speeche* (1941).

Rosato, S. *Europe United: Power Politics and the Making of the European Community* New York: Cornell University Press, 2011.

Rosenberg, J. . "Security in Embedded Systems ". In *Rugged Embedded Systems* edited by A. Bose Vega, P. Burlington: Morgan Kaufmann, 2017.

Ross, R.S. "The 1995-96 Taiwan Strait Confrontation: Coercion, Credibility and the Use of Force". *International Security* 25, no. 2 (2000): 87-123.

Routley, N. "Mapped: All the World's Military Personnel": Visual Capitalist 2022.

Roy, D. *Taiwan: A Political History* Ithaca: Cornell University Press 2003.

Ruggie, J.G. . "What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge". *International Organization* 52, no. 4 (1998): 855-85.

Russia. "Conceptual View Regarding the Activities of Armed Forces of the Russian Federation in Information Space ": Russian Federation 2011.

———. "Doctrine of Information Security of the Russian Federation": Russian Federation, 2016.

Rusten, J.S. . *Thucydides* Oxford: Oxford University Press, 2009.

S., Watts. "A More Peaceful World? Regional Conflict Trends and Us Defnece Planning ": RAND 2017.

Saeed, I., A. Selmat, and A. Abuagoub. "A Survey on Malware and Malware Detection Systems". *International Journal of Computer Applications* (April 2013).

Sagromoso, D. . "Who 'Defeated' Isis? An Analysis of Us and Russian Contributions". *Russia Matters* (6 May 2020).

Salama, I. . "Human Rights Diplomacy from a Un Perspective: A Complement to Advocacy." In *Human Rights Diplomacy: Contemporary Perspectives* edited by M. O'Flaherty, 129-53. Netherlands: Brill Nijhoff, 2011.

Salamon, L.M. . "The Rise of the Non-Profit Sector". *Foreign Affairs* 73, no. 4 (1992): 109-22.

Salem, M.B., S. Hershkop, and S. J. Stolfo. "A Survey of Insider Attack Detection Research." In *Insider Attack and Cyber Security* edited by S.J. Stolgo, 69-90 Boston: Springer Science and Business Media, 2008.

Salm, K. . "Baltic States Need More Nato Forces to Deter a Russian Invasion, Says Estonian Official." By J. Grady. *USNI News* (16 June 2022).

Samaan, J. . "From War to Deterrence? Israel-Hezbollah Conflict since 2006". *Strategic Studies Institute, US Army War College* (2014).

Sanders, P. . "Britain Has Offensive Cyberwar Capability, Top General Admits'." By D. Sabbagh. *The Guardian* (25 September 2020).

Sandler, S. *The Korean War: No Victory, No Victors, No Vanquished* Kentucky Kentucky University Press 1999.

Sanger, D. "China Appears to Warn India: Push Too Hard and the Lights Could Go Out", *The New York Times* 28 February 2021.

Sanger, D.E., and W.J. Broad. "Trump Inherits a Secret Cyberwar against North Korean Missiles", *The New York Times*, 4 March 2017.

Sarbin, T.R., and V.L. Allen. "Role Theory." In *The Handbook of Social Psychology*, edited by Lindzey. G. and E. Aronson. Reading MA: Addison-Wesley, 1968.

Sauer, P. "Putin Flirts Again with Grim Prospect of Nuclear War – This Time He Might Mean It", *The Guardian*, 21 September 2022.

Schachter, O. . "The Decline of the Nation-State and It Implications for International Law". *Columbia Journal of Transnational Law* 36 (1998): 7-25.

Scharre, P. . "Autonomous Weapons and Operational Risk". *Centre for a New American Security* (February 2016).

Scheuerman, W.E. . *Hans Morgenthau: Realism and Beyond* Malden, MA: Polity, 2009.

Schmidt, B. . "International Relations Theory: Hegemony or Pluralism?". *International Relations Theory* 36, no. 2 (2007): 105-14.

Schmidt, M.S., D.E. Sanger, and N. Perlroth. "Chinese Hackers Pursue Key Data on Us Workers", *The New York Times* 7 March 2014.

Schmitt, M.N. . *Tallinn Manual on the International Law Applicable to Cyber Warfare* Cambridge: Cambridge University Press, 2013.

Schmitt, M.N., and B.T O'Donnell. "Foreword – Computer Network Attack and International Law". *International Law Studies* 76 (2002).

Schrader, J, Y. , L. Lewis, and R.A. Brown. "Quadrennial Defence Review (Qdr) Analysis: A Retrospective Look at Joint Staff Participation ": RAND 1999.

Schuman, M. "What Happens When China Leads the World". *The Atlantic* (5 October 2020).

Schwab, K. . *The Fourth Industrial Revolution* New York: Crown, 2016.

Schwartau, W. "Hearing before the Subcommittee on Technology and Competitiveness on Computer Security": US Congress, 1991.

Scott, J.A. *Matter of Record.* Cambridge: Polity Press, 1990.

Securicon. "What's the Difference between Ot, Ics, Scada and Dcs", 2019.

Segrè, C.G. . "Giulio Douhet: Strategist, Theorist, Prophet?". *The Journal of Strategic Studies* 15, no. 3 (1992): 351-66.

Sembiring, Z. . "Stuxnet Threat Analysis in Scada (Supervisory Control and Data Acquisition) and Plc (Programmable Logic Controller) Systems". *Journal of Computer Science, Information Technology and Telecommunications Engineering* 1, no. 2 (2020): 96-103.

Sepulveda, E., Smith, H. . "Technological Challenges of Stealth Unmanned Combat Aerial Vehicles". *The Aeronautical Journal* 121, no. 1243 (2017): 1261-95.

Services, Congressional Committee on the Armed. "The Committee's Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain", edited by US Congress, 2011.

Seuronix. "Insider Threat Survey Report ", 2019.

———. "Insider Threats: Why It Continues to Matter Today", 2020.

Sevastopulo, D. "Chinese Intelligence Officer Convicted of Stealing Secrets from Ge", *Financial Times* 5 November 2021.

Seversky, A. *Victory through Air Power.* New York: Simon and Schuster, 1942.

Shalal-Esa, A. . "Lockheed's F-35 Logistics System Revolutionary but Risky", *Reuters*, 16 November 2012.

Sharwood, S. "Us Energy, Nuke and Aviation Sectors under Sustained Attack". *The Register* (22 October 2017).

Shattuck, T.J. "The Race to Zero?: China's Poaching of Taiwan's Diplomatic Allies". *Orbis* 64, no. 2 (2020): 334-52.

Sheffield, G. . "From San Carlos to Stanley: The Falklands Land/Air Operation". *International Relations* 20, no. 3 (2006): 370-75.

Shiner, L. . "F-35: What the Pilots Say", *Air and Space Magazine*, April 2019.

Shlapak, D.A., and M.W. Johnson. *Reinforcing Deterrence on Nato's Eastern Flank: Wargaming the Defense of the Baltics.* Santa Monica: RAND, 2016.

Sil, R., and P.J. Katzenstein. *Beyond Paradigms: Analytic Eclecticism in the Study of World Politics.* Basingstoke: Palgrave MacMillan, 2010.

Simmonds, A., P. Sandilands, and L. van Ekert. "An Ontology for Network Security Attacks", In *Asian Applied Computing Conference*, 317-23, 2004.

Simmons, D. "Cyber-Attacks 'Damage' National Infrastructure", *BBC News* 5 April 2019.

Simmons, J.A. *Locke, Consent and the Limits of Society* Princetown Princetown University Press, 1993.

Simon, L. "Demystifying the A2ad Buzz". *War on the Rocks* (4 January 2017).

Simpson, J. . "Russia's Crimea Plan Detailed, Secret and Successful", *BBC News Online*, 19 March 2014.

Singer, P.W., and A. Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know* Oxford Oxford University Press, 2014.

Skinglsey, J. . "The Solarwinds Hack: A Valuable Lesson for Cybersecurity". *Chatham House* (2 February 2021).

Skowronski, W. . "Vulnerability in Cyberspace", *Air Force Magazine*, December 2016.

Smith, D.J. . "Russian Cyber Capabilities, Policy and Practice". *Contemporary Conservative Thought* Winter (2014).

Smith, M. E. . "The Strategic Bombing Debate: The Second World War and Vietnam". *Journal of Contemporary History* 12 (1977): 175-91.

Snow, S. "This Is How the Us Military Is Protecting the Strait of Hormuz", *Military Times* 29 December 2019.

Snowdon, E. "Edward Snowdon / Twitter Account", edited by TheTrueHOOHA, 2013.

Snugg, L. "Spending Review: Backlash over Rishi Sunak's Overseas Aid Cut." By BBC News Online. *BBC* (2020).

Snyder, J. L. "The Soviet Strategic Culture: Implications for Limited Nuclear Operations": RAND, 1977.

Soesanto, S. "The Evolution of Us Defense Strategy in Cyberspace (1988 – 2019)". *Cyber Defense Project, Center for Security Studies* (August 2019).

Software.Informet. "Skygrabber 2.6 ", 2021.

Sohalianwar, S. . "Point to Point Topology; Advantages and Disadvantages". *Computer Technology Topology* (20 August 2019).

SolarWinds. "Cert Advisory: Vulnerability Report", 2021.

———. "Leader in Network Management Software and Monitoring Tools", 2021.

Soliman, M. "Home Drones Are Re-Engineering the Geopolitics of the Middle East Drones Are Re-Engineering the Geopolitics of the Middle East". *Middle East Institute* (7 March 2022).

Solomon, G.B. *The Nato Enlargement Debate, 1990-1997.* Westport Praeger 1998.

Soone, P. "Battle for Kyiv: Ukrainian Valor, Russian Blunders Combined to Save the Capital", *The Washington Postg*, 24 August 2022.

Splunk. "It Security Predictions 2020", 2020.

———. "Threat Update: Acidrain Wiper": Splunk, 2022.

Sprout, H., Sprout, M. . "Environmental Factors in the Study of International Politics". *The Journal of Conflict Resolution* 1, no. 4 (December 1957): 309-28.

Srinivasan, K. . *The Rise, Decline and Future of the British Commonwealth* Basingstoke: Palgrave MacMillan, 2005.

Staff-Writer. "China Protests Us Spy Plane Watching Drills", *Reuters*, 25 August 2020.

———. "The Future of Automoation in the Aviation Industry". *Robotics & Automoation* (2019).

———. "The Gulf War: A Chronology". *Air Force Magazine* (1 January 2001).

———. "India-China Dispute: The Border Row Explained", *BBC News Online*, 25 January 2021.

———. "'It Was Human Error': Cyberattacks Too Place but Didn't Cause Mumbai Outage Says Govt", *The Times of India*, 2 March 2021.

———. "Mumbai Power Outage in October May Have Been Result of 'Cyber Sabotage'", *The Wire* 2 March 2021.

———. "Patriot Missile Long-Range Air-Defence System". *Army Technology* (November 2020).

———. "Practice Disconnected". *Armed Forces Journal* (1 December 2012).

———. "Russia Moved 80% of Troops from Nato Borders to Ukraine", *Rubryka*, 29 September 2022.

———. "When Will Sweden and Finland Join Nato? Tracking the Ratification Process across the Alliance". *Atlantic Council* (27 September 2022).

Staff, Reuters. "Timeline: Taiwan's Road to Democracy", *Reuters* 13 December 2011.

StaffWriter. "Hacked: How China Stole Us Technology for Its J-20 Stealth Fighter", *National Interest*, 10 July 2019.

Statista.com. "Forecast of Social Network User Numbers in the United Kingdom (Uk) from 2015 to 2022 (in Million Users) ", 2018.

Statistica. "The 15 Countries with the Highest Military Spending Worldwide in 2019."

Steinnon, R. . "Cyber Pearl Harbour Versus the Real Pearl Harbor", *Forbes* 7 December 2017.

Stephenson, C. . *Zeppelins: German Airships 1900? .* Oxford: Osprey Publishing, 2005.

Sterling-Folker, J. "Realist-Constructivism and Morality". *International Studies Review* 6, no. 2 (2004): 341-52.

Stewart, P. "Exclusive: U.S. Seeks Way to Speed Delivery of New Fighter Jets to Taiwan", *Reuters*, 20 January 2022.

Stoica, A. "Social Engineering as the New Deception Game". *Romanian Journal of Information Technology and Automatic Contr* 31, no. 3 (2021): 57-68.

Stoltenberg, J. "Russia’s Neighbors Fear Nato’s Defense Plans Are Not Fit for Purpose and They Could Be Quickly Overrun." By S. Meredith. *NBC* (2022).

Stone, M. . "Us to Sell 34 Surveillance Drones to Allies in the South China Sea Region", *Reuters*, 3 June 2019.

Stoneburner, G., A. Goguen, and A. Feringa. "Risk Management Guide for Information Technology Systems: Recommendation of the National Institute of Standards and Technology ", In *Special Publication 800-30*: National Institute of Standards and Technology 2002.

Strohmeier, M., V. Lenders, M. Schafer, I. Martinovic, and M. Smith. "Assessing the Impact of Aviation Security on Cyber Power", In *8th International Conference on Cyber Conflict*: NATO CCDCOE 2016.

Suciu, P. "Tempest: The Revolutionary Stealth Fighter That Might Be Too Expensive". *National Interest* (5 March 2021).

Suciu, P. . "Is the Uk Considering Cutting Its Order for the F-35?", *The National Interest*, 13 March 2021.

Suggs, L. "Uk Curbs Global Britain Ambitions as Coronavirus Bites." By C. Gallardo (25 November 2020).

Sun, Y. "How China Could Cyberattack Taiwan." By R. Jennings (10 December 2021).

Suskind, R. . *The One Percent Doctrine: Deep inside America's Pursuit of Its Enemies since 9/11.* New York: Simon & Schuster, 2006.

Szmigiera, M. "Countries with the Highest Military Spending 2020": Statistica, 2021.

Tabatabai, A.M., Martinin, J., Wasser, B. "The Iran Threat Network (Itn): Four Models of Iran's Nonstate Client Partnerships". (2021).

Tambini, O. . "Black Friday Vs Cyber Monday: What's the Difference?", *Techradar*, 14 November 2019.

Tariq, N., M. Asim, and F.A. Khan. "Securing Scada-Based Critical Infrastructure: Challenges and Open Issues", In *5th International Workshop on Cyber Security and Digital Investigation*, 2019.

Tarnoff, B. "How the Internet Was Invented", *The Guardian* 15 July 2016.

Tarschys, D. "The Council of Europe: 50 Years of European Cooperation". *European Review* 7, no. 5 (1999): 497-507.

Taylor, A. . "Operation Desert Storm: 25 Years since the First Gulf War", *The Atlantic*, 14 January 2016.

Taylor, M. "Lost Laptops, Disks and Dossiers", *Independent*, 15 June 2008.

TCH. "Due to a Hacker Attack, the Power of Half the Ivano-Frankivsk Region Was De-Energised." TCH Online, https://translate.google.co.uk/translate?hl=en&sl=ru&u=https://ru.tsn.ua/ukrayin a/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti550406.html&prev=search.

Team, Threat Intelligence. "Tortoiseshell Group Targets It Providers in Saudi Arabia in Probable Supply Chain Attacks": Symantec 2019.

Technologies, Egress Software. "Insider Data Breach Survey ", 2019.

Technology, National Institute of Standards and. "Nist 800-30 – Guide for Conducting Risk Assessments", 2012.

Techopedia. "Air Gap " https://www.techopedia.com/definition/17037/air-gap.

———. "Computer Systems ", 2018.

———. "Faraday Cage", 2019.

———. "Hardening ", 2020.

TechTerms. "Computer Chip", In *Hardware Terms* 2018.

Tegler, E. "U.S. Navy Just Got Its First New F/a-18 Super Hornets — Here Are the Key Upgrade", *Forbes* 22 June 2020.

Teng, J. "Taiwan in the Chinese Imagination, 17th-19th Centuries". *The Asia-Pacific Journal* 5, no. 6 (4 June 2007): 1-31.

"Territorial Disputes in the South China Sea - Global Conflict Tracker". edited by Council of Foreign Relations, 2020.

Textor, C. . "Taiwan - Statistics and Facts ": Statistica, 2001.

The-Courage-Foundation. "Who Is Edward Snowdon? ." https://edwardsnowden.com/

Thim, M. . *Taiwan's Air Force: Inventory and Procurement Options.* Taiwan in Perspective 2013.

Thompson, D. "Hope on the Horizon: Tawian's Radical New Defense ". *War on the Rocks* (2 October 2018 2018).

Thomson, I. "Everything You Need to Know About the Petya, Er, Notpetya Nasty Trashing Pcs Worldwide". *The Register* (28 June 2017).

Thornton, R. and Miron, M. "Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constrains Faced by the United Kingdom". *Journal of Cyber Policy* 4, no. 2 (2019): 257-74.

Thucydidies. *The History of the Peloponnesian War.* Translated by R. Crawley. New York: Dutton and Company.

Tidy, J. "Ukraine Cyber-Attack: Russia to Blame for Hack, Says Kyiv", *BBC News* 14 January 2022 2022.

Tidy, J. . "Solarwinds: Why the Sunburst Hack Is So Serious", *BBC News Online*, 16 December 2020.

Tilford, E. "Operation Allied Force and the Role of Air Power". *Parameters* Winter (2000): 24-38.

Tirpak, J.A. "The Chinese Air Force's Great Leap Forward". *Air Force Magazine* (29 May 2018).

———. "Next National Defense Strategy Should Return to Two-War Force Construct", *Air Force Magazine* 15 June 2021.

Toft, B., and S. Reynolds. *Learning from Disasters – a Management Approach.* Leicester: Perpetuity Press, 1997.

Townshead, C. "The League of Nations and the United Nations", *BBC History* 2017.

Trenchard, H. "The Effect of the Rise of Air Power on War", edited by Air Ministry Directorate of Staff Duties. London: UK, 1946.

Trenin, D. . "Russia's Line in the Sand on Syria: Why Moscow Wants to Halt the Arab Spring ". *Foreign Affairs* (5 February 2012).

Trevor-Roper, H.R. . *Hitler's War Directives: 1939-1945* London: Sidgwick and Jackson, 1964.

Tri, N. "China's A2/Ad Challenge in the South China Sea: Securing the Air from the Ground". *The Diplomat* (19 May 2017 2017).

Trimble, S. "U.S. Air Force Talks New F-16 Orders in Latest Acquisition Shake-Up", *Aviation Week*, 21 January 2021.

Trump, D. "Iran Nuclear Deal: Trump Pulls Us out in Break with Europe Allies." By Staff Writer. *BBC News* (2018).

———. "Trump Threatens 'Delinquent' Nato Allies with Trade Blocks If They Don't Meet Military Spending Targets." By A. Woodward (3 December 2019 2019).

Tsai, I. . "Inaugural Address of Roc 15th-Term President Tsai Ing-Wen", edited by President of Taiwan, 2020.

Tsirbas, M. . "What Does the Nine-Dash Line Actually Mean?". *The Diplomat* (2 June 2016).

Tuckness, A. . "Lockes Political Philosophy." In *Stanford Encyclopaedia of Philosophy* edited by E.N. Zalta. Stanford Stanford University Press, 2005.

Typhoon, Eurofighter. "Our History", 2021.

Tyugu, E. "Command and Control of Cyber Weapons", In *4th International Conference on Cyber ConÀ ict*. Tallin 2012.

Tzu-ti, H. "Taiwan's National Power Company Hit by Cyberattacks on Daily Basis", *Taiman News*, 6 December 2021 2021.

Tzu, S. . *Art of War* Translated by L. Giles. Leicester: Allandale Online, 400-200 BC.

UK. "Aviation Cyber Security Strategy: Moving Britain Ahead", edited by Department for Transport, 2018.

———. "Battle of Britain ", edited by Royal Air Force. Great Britain 2020.

———. "Combat Air Strategy: An Ambitious Vision for the Future ", edited by Ministry of Defence, 2018.

———. "Critical National Infrastructure ", edited by Centre for the Protection of National Infrastructure, 2018.

———. "Current Trade Sanctions, Including Arms Embargoes and Other Restrictions", edited by Department for International Trade. Great Britain HM Government 2020.

———. "Cyber Essentials: Technical Controls ": National Cyber Security Centre, 2020.

———. "Cyber Primer", edited by Ministry of Defence, 2016.

———. "Defence in a Competetive Age", edited by Minostry of Defence, 2021.

———. "Finance and Economics Annual Statistical Bulletin: International Defence 2019 ", edited by Ministry of Defence, 2019.

———. "The Fundamentals of Risk ": . National Cyber Security Centre, 2019.

———. "Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy", edited by HM Government, 2021.

———. "Government End User Device Strategy": HM Government 2011.

———. "Government Outsourcing: What Has Worked and What Needs Reform? ", edited by Institute for Government: HM Government 2019.

———. "Hms Ia Standard Numbers 1 and 2: Information Risk Management", 2012.

———. "How Spies Operate ": Security Service (MI5), 2020.

———. "Integrated Operating Concept (Iopc)", edited by Ministry of Defence, 2021.

———. "Intelligence and Security Committee of Parliament: Annual Report, 2019-2021", edited by House of Commons, 2021.

———. "International Development Act", edited by HMG, 2015.

———. "Joint Concept Note 1/20 - Multi-Domain Integration", edited by Ministry of Defence, 2020.

———. "Joint Concept Note (Jcn) 2/17 – Future of Command and Control", edited by Ministry of Defence, 2017.

———. "Joint Defence Doctrine 0-01 Uk Defence Doctrine", edited by Defence Concepts and Doctrine Centre. : Ministry of Defence, 2014.

———. "Joint Doctrine Note 1/18 - Cyber and Electromagnetic Activities", edited by Ministry of Defence, 2018.

———. "Joint Doctrine Publication 0-30: Uk Air and Space Power, 2nd Ed", edited by Concepts and Doctrine Centre. Great Britain Ministry of Defence Defence, 2017.

———. "Joint Service Publication (Jsp) 441 – Managing Information in Defence – Part 1: Directive": Ministry of Defence 2017.

———. "Joint Tactics, Techniques and Procedures 4-05: Operational Infrastructure", edited by Ministry of Defence: Development, Concepts and Doctrine Centre (DCDC), 2012.

———. "Jsp 536 - Defence Research Involving Human Participants", edited by Ministry of Defence, 2022.

———. "Lightening (F35-B) (2021)", edited by Royal Air Force, 2021.

———. "Ministry of Defence - the Equipment Plan 2020 to 2030", edited by National Audit Office, 2021.

———. "Ministry of Defence Research Ethics Committee", edited by Ministry of Defence, 2022.

———. "National Cyber Force Explainer ", edited by National Cyber Force, 2021.

———. "National Cyber Security Strategy", edited by Cabinet Office: HM Government 2016.

———. "National Security Strategy and Strategic Defence and Security Review: A Secure and Prosperous United Kingdom", edited by HM Government. Great Britain HM Government, 2015.

———. "Operation Kipion", edited by Royal Navy, 2022.

———. "The Orange Book: Management of Risk – Principles and Concepts", 2019.

———. "Penetration Testing ": National Cyber Security Centre, 2019.

———. "Persuasion and Power in the Modern World - Select Committee on Soft Power and the Uk's Influence", edited by Select Committee on Soft Power, 2014.

———. "Policy Paper: Regulation for the Fourth Industrial Revolution - Energy and Industrial Strategy", edited by Secretary of State for Business, 2019.

———. "Protector (Rg Mk 1)", edited by Royal Air Force, 2021.

———. "Reaper (Mq-Ra)", edited by Royal Air Force, 2-21.

———. "Russia Behind Cyber-Attack with Europe-Wide Impact an Hour before Ukraine Invasion", edited by Gov.UK, 2022.

———. "Science and Technology Strategy", edited by Ministry of Defence, 2020.

———. "Sdsr 2015: Defence Fact Sheets, Defence Strategy and Priorities", edited by HM Government. Great Britain Ministry of Defence 2016.

———. "Spending Review 2020", edited by HM Treasury, 2020.

———. "Spending Review: Reducing the 0.7% Aid Commitment", edited by House of Commons Library, 2020.

———. "A Strong Britain in an Age of Uncertainty: The National Security Strategy", edited by HM Government, 2010.

———. "Supply Chain Security Guidance ", edited by National Cyber Security Centre, 2020.

———. "Tempest", edited by Royal Air Force, 2021.

———. "Tempest Aircraft Concept ", edited by Royal Air Force, 2021.

———. "Uk and Sweden Partner on Future Combat Air', Defence and Armed Forces News Story", edited by Gov.UK. Defence and Armed Forces News Story 2019.

———. "The Uk Cyber Security Strategy Protecting and Promoting the Uk in a Digital World", edited by Cabinet Office: HM Government 2011.

———. "Uk, Us and Australia Launch New Security Partnership", edited by.Gov.UK, 2021.

———. "Vulnerability Management ", edited by National Cyber Security Centre, 2022.

Ukraine. "Cyber Security Strategy of Ukraine", edited by President of Ukraine, 2016.

Ullman, H. . "War in Iraq: Shock and Awe Revisited". *The RUSI Journal* 148, no. 3 (2003): 10-14.

Ullman, R. . "Redefining Security". *International Security* 8, no. 1 (1983): 129-53.

UN. "2005 World Summit Outcome Document ", 2005.

———. "2222 (Xxi) – Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space": United Nations, 1966.

———. "Charter of the United Nations – Chapter I: Purposes and Principles, Article 2 ", 1945.

———. "Charter of the United Nations – Chapter Vii: Action with Respect to Threats to Peace, Breaches of the Peace and Acts of Aggression, Article 39 ", 1945.

———. "Oceans and Law of the Sea. The United Nations Convention on the Law of the Sea", 1988.

———. "Security Council, Resolution 1540", 2004.

———. "Un Charter ", 1945.

Unit, Digital Security. "Special Report: Ukraine - an Overview of Russia's Cyberattack Activity in Ukraine ": Microsoft 2022.

Unknown. "Estonian Foreign Ministry Memo." In *The Baltic States and the End of the Cold War*, edited by K. Piirimäe, Mertelsmann, O. , 224-31. Berlin: Peter Lang, 1993.

———. "Rq-170 Sentinel Drone Downed in Iran Critical Updates!", In *Aviationintel.com*, 2011.

Urkandu, E., Ben-Farah, M., Hindy, H. . "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends". *Information System Frontiers*, no. 13 (2022): 146-68.

US. "Air Based Technologies", edited by DHS Science and Technology Directorate: Department of Homeland Security 2017.

———. "Air Force Furute Operating Concept: A View of the Air Force in 2035", edited by US Air Force, 2015.

———. "Alert (Aa21-042a) – Compromise of Us Water Treatment Facility", edited by Cybersecurity & Infrastructure Security Agency (CISA), 2021.

———. "Alert (Aa21-201a): Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013", edited by Cybersecurity and Infrastructure Security Agency (CISA), 2021.

———. "Alert (Ir-Alert-H16-056-01), Cyber-Attack against Ukrainian Critical Infrastructure", edited by Department of Homeland Defence: International Control Systems Computer Emergency Response Team, 2016.

———. "Alert (Ta18-074a) - Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, 15 March (2018)", edited by the Office of the Director of National Intelligence (ODNI) and the National Security Agency (NSA) Cybersecurity and Infrastructure Security Agency (CISA), 2018.

———. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019", edited by US Department of Defense, 2019.

———. "Audit of the Dod's Management of the Cybersecurity Risks for Government Purchase of Commercial Off-the-Shelf Items", edited by Inspector General of the US Department of Defence, 2019.

———. "China's Economic Rise: History, Trends, Challenges, and Implications for the United States", edited by Congressional Research Service, 2019.

———. "Chinese Nationalist Maritime Activities against the China Mainland", edited by National Security Archive, 1962.

———. "Cybersecurity Advisory - Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities ", edited by National Security Agency (NSA), 2020.

———. "Cybersecurity Advisory - Chinese State-Sponsored Cyber Operations: Observed Ttps", edited by Cybersecurity and Infrastructure Security Agency (CISA) National Security Agency (NSA), Federal Bureau of Investiation (FBI), 2021.

———. "Data Network Evaluation Criteria Handbook", edited by Federal Aviation Authority, 2009.

———. "Defense Primer: United States Airpower", edited by Congressional Research Service, 2021.

———. "Department of Defense Authorization for Appropriations for Fiscal Year 2013", edited by US Congress, 2014.

———. "Dod Inspector General Report on Excessive Profits by Transdigm Group, Inc'", edited by Department of Defence: Inspector General 2019.

———. "Eisenhower Carrier Strike Group Enters 5th Fleet", edited by UN Naval Forces Central Command Public Affairs, 2021.

———. "Eligible Receiver 97", edited by Department of Defense, 1997.

———. "F-35 Joint Strike Fighter (Jsf) ", edited by Office of the Secretary of Defense, 2022.

———. "F-35 Joint Strike Fighter (Jsf) Program", edited by US Congressional Research Service, 2022.

———. "F-35 Joint Strike Fighter Fy 17 Department of Defence Projects ", edited by Operational Test and Evaluation, 2018.

———. "F-35 Sustainment: Enhanced Attention to and Oversight of F-35 Affordability Are Neede", edited by US Government Accountability Office, 2021.

———. "Faa Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to Nextgen", edited by Goverment Accountability Office, 2015.

———. "Foreign Relations of the United States and China, 1964–1968", edited by Office of the Historian, 2022.

———. "Global Trends 2030: Alternative Worlds", edited by National Intelligence Council, 2012.

———. "Global Vigilance, Global Reach, Global Power for America", edited by US Air Force, 2013.

———. "Identifying at-Risk Employees: A Behavioural Model for Predicting Potential Insider Threats", edited by Department of Energy, 2010.

———. "Interim National Security Strategic Guidance ", edited by White House, 2021.

———. "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World", edited by President of the United States, 2011.

———. "Iran - Current Topics", edited by National Security Agency (NSA). The Intercept 2015.

———. "Joint Statement by the Federal Bureau of Investigation (Fbi)", edited by the Office of the Director of National Intelligence (ODNI) and the National Security Agency (NSA) Cybersecurity and Infrastructure Security Agency (CISA), 2021.

———. "Keynote Address by Secretary of Defense Mark T. Esper at the Reagan National Defense Forum", edited by US Department of Defense, 2019.

———. "Military and Security Developments Involving the People's Republic of China 2020", edited by US Department of Defense, 2020.

———. "Military and Security Developments Involving the People's Republic of China - Annual Report to Congress", edited by Department of Defence, 2021.

———. "Missile Defence Review (2019)", edited by Department of Defence, 2019.

———. "Modernizing Us Air Space: Next Generation Air Transportation", edited by Federal Aviation Authority, 2020.

———. "Monroe Doctrine, 1823", edited by Office of the Historian, 2022.

———. "National Defence Strategy of the United States of America ", 2018.

———. "National Defense Authorization Act for Fiscal Year 2022", edited by US Congress, 2021.

———. "National Military Strategy for Cyberspace Operations", edited by Department of Defence, 2003.

———. "National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat", edited by Department of Homeland Security: National Protection and Programs Directorate Office of Infrastructure Protection, 2013.

———. "National Security Strategy", edited by President of the United States, 2010.

———. "The National Security Strategy", edited by National Security Council, 2002.

———. "National Security Strategy of the United States of America", edited by President of the United States, 2017.

———. "National Strategy for Aviation Security of the United States of America", edited by President of the United States, 2018.

———. "The National Strategy to Secure Cyberspace", edited by White House, 2003.

———. "Observations on the Marine Corps F-35b Demonstration on Uss Wasp: Memorandum for under Secretary of Defense for Acquisition, Technology and Logistics", edited by Operational Test and Evaluation, 2015.

———. "Office of Special Investigations Guidance - Travelling with Laptops and Mobile Devices", edited by US Air Force, 2017.

———. "Operation Inherent Resolve: Target Operations to Defeat Isis", edited by United States Department of Defence, 2017.

———. "The Opm Data Breach: How the Government Jeopardised Our National Security for More That a Generation", edited by US House of Representatives Oversight and Government Reform Committee, 2016.

———. "Poison Ivy ", edited by State of New Jersey. NJCCIC Threat Profile, 2017.

———. "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs: Memorandum for Commander Army Test and Evaluation Command and Air Force Operational Test and Evaluation Centre", edited by Operational Test and Evaluation, 2014.

———. "Providing for the Common Defense", edited by National Defense Strategy Commission, 2018.

———. "Quadrennial Defense Review", edited by Historical Office of the Secretary of Defense, 2022.

———. "Readout of President Joe Biden's Meeting with Prime Minister Rishi Sunak of the United Kingdom", edited by The White House, 2022.

———. "Readout of President Joseph R. Biden Jr.'S Meeting with Prime Minister Boris Johnson of the United Kingdom", edited by The White House, 2021.

———. "Renewed Great Power Competition: Implications for Defense—Issues for Congress", edited by Congressional Research Service, 2022.

———. "Resilient Military Systems and the Advanced Cyber Threat", edited by Department of Defense Defense Science Board, 2013.

———. "Review of the Unauthorised Disclosure by Former National Security Agency Contractor Edward Snowden", edited by House of Representatives, 2016.

———. "Snowdon – Preliminary Hearing Transcript", edited by Senate: Senate Committee on Homeland Security and Governmental Affairs, 2013.

———. "Southeast Asia Treaty Organization (Seato), 1954", edited by Office of the Historian, 2022.

———. "Statement on Formosa", edited by US State Department, 1950.

———. "Taiwan Allies International Protection and Enhance Initiative (Taipei) Act ", edited by US Congress, 2019.

———. "The Taiwan Straits Crises: 1954–55 and 1958", edited by The Office of the Historian, 2022.

———. "U.S. Conducts First Hunt Forward Operation in Lithuania", edited by US Cyber Command, 2022.

———. "Understanding Denial-of-Service Attacks', Security Tips", edited by Cyber-Security & Infrastructure Agency, 2009.

———. "The United States Strategic Bombing Survey: Summary Report", edited by United States Air Force, 1945.

———. "Us-China Strategic Competition in South and East China Seas: Background and Issues for Congress", edited by Congressional Research Service: US Congress, 2020.

———. "Us China Economic and Security Review Commission: 2015 Report to Congress", edited by United States Congress, 2015.

———. "Us District Court Western District of Pennsylvania - Us Vs Yuriy Andrienko ", 2020.

———. "Us Relations with Germany", edited by US DEpartment of State, 2022.

Utley, M. "Royal Navy's Biggest Warship, Hms Queen Elizabeth, in New York to Sink Cybersecurity Threats." By D. Winder. *Forbes* (21 October 2018).

Vann Woodward, C "The Age of Reinterpretation". *American Historical Review* 66 (1960).

Varadarajan, L. "Constructivism, Identity and Neoliberal (in)Security". *Review of International Studies* 30 (2004): 319-41.

Vatanka, A. "A New Chapter for Iran and Russia". *Foreign Policy* (21 January 2022).

Veebel, V. . "Nato Options and Dilemmas for Deterring Russia in the Baltic States". *Defence Studies* 18, no. 2 (2018): 229-51.

Venhuizen, H. . "Air Force C-17s Delivering Relief to Beirut Following Deadly Explosions’", *Military Times*, 2020.

Viasat. "Ka-Sat Network Cyber Attack Overview", 2022.

Vincent, J. . "The Hobbesian Tradition in Twentieth Century International Thought". *Journal of International Studies* 10, no. 2 (1981): 91-101.

Volgy, T.J., R. Corbetta, K. A. Grant, and R. G. Baird. *Major Powers and the Quest for Status in International Politics: Global and Regional Perspectives* New York: Palgrave MacMillan, 2011.

VonKuhlmann, R. . "The Permanent Bases of German Foreign Policy". *Foreign Affairs* 9, no. 2 (January 1931): 179-94.

Voo, J., I. Hemani, S. Jones, W. DeSombre, D. Cassidy, and A. Schwarzenback. "National Cyber Power Index 2020": Belfer Center, 2020.

Waever, O. . "Four Meanings of International Society: A Trans-Atlantic Dialogue." In *International Society and the Development of International Relations Theory* edited by B.A. Roberson, 85-89. London: Pinter, 1998.

Wallace, W., Phillips, C. . "Reassessing the Special Relationship". *International Affairs* 5, no. 2 (2009): 263-84.

Walt, S.M. "Nato Owes Putin a Big Thank You ". *Foreign Policy* (4 September 2014).

———. "The Renaissance of Security Studies". *International Studies Quarterly* 35, no. 2 (1991): 211-39.

Walt, S.M. . "International Relations: One World, Many Theories". *Foreign Policy* 110 (1998): 29-46.

Waltz, K.N. "The Origins of War in Neorealism Theory". *Journal of Interdisciplinary History* 18, no. 4 (1988): 615-28.

Waltz, K.N. . *Theory of International Politics* Reading MA: Addison-Wesley Publishing Company, 1979.

Ward, T.J., Lay, W.D. "The Unusual Case of Taiwan". *e-International Relations* (1 May 2019).

Warden, J.A. "Strategy and Airpower". *Air and Space Power Journal* Spring (2011): 64-77.

Warrell, H. . "Mod Accused of Overspending as Budget ‘Black Hole’ Hits £17bn", *Financial Times* 21 January 2021.

Warren, C. . "Statement before the Subcommittee on Commerce, Justice, State and Judiciary." In *The Clinton Record on Democracy Promotion*, edited by T. Carothers: Carnegie Endowment for International Peace, 1992.

Wege, C.A. "Iranian Counterintelligence". *International Journal of Intelligence and CounterIntelligence* 32, no. 2 (9 May 2019): 272-94.

Weiner, N. . *Cybernetics: Control and Communication in the Animal and the Machine* Cambridge, MA: MIT Press, 1948.

Weisgerber, M. . "Us Preparing to Put Nuclear Bombers Back on 24-Hour Aler", *Defence One*, 22 October 2017.

Welby, J. . "Archbishop of Canterbury: Uk Must Keep Its Foreign Aid Promises", *Financial Times*, 2020.

Wendt, A. "Anarchy Is What States Make of It: The Social Construct of Power Politics". *International Organization* 46, no. 2 (1992): 391-425.

Wendt, A. . *Social Theory of International Politics.* Cambridge Cambridge University Press, 1999.

Wharton, J. "What Is the Joint Expeditionary Force?", *Forces.net*, 14 March 2022.

Wheeler, T. . "In Cyberwar, There Are No Rules: Why the World Desperately Needs Digital Geneva Conventions". *Foreign Policy* (12 September 2018).

Wight, M. . *System of States.* Leicester Leicester University Press, 1977.

Wigston, M. "Key Note Speech ", In *Global Air Chiefs Conference*, 2021.

Wigston, M. . "Trenchard Memorial Lecture". *RUSI* (January 2021).

Willett, M. . "Assessing Cyber Power". *Survival* 61, no. 1 (2019): 85-90.

Williams, A.J. . "A Crisis in Aerial Sovereignty? Considering the Implications of Event Military Violations of National Airspace". *Area* 42, no. 1 (2010): 51-59.

Williams, B.D. "Cybercom Has Conducted 'Hunt-Forward' Ops in 14 Countries, Deputy Says", *Breaking Defense*, 10 November 2021.

Williams, Z. . "China's Tightening Grasp in the South China Sea: A First Hand Look", *The Diplomat*, 10 June 2020.

Wilson, E.J. . "Hard Power, Soft Power, Smart Power". *The Annals of the American Academy of Political and Social Science* 616 (2008): 110-24.

Wilson, H. "Key Piece of F-35 Logistics System Unusable by Us Air Force Students, Instructor Pilots." By V. Insinna. *Defence News* (8 March 2019 2019).

Wilson, M. . "Silicon Wafer Makers Plan 20% Increase in Price in 2018". *Kit Guru.net* (5 February 2018).

Wilson, P. . "Idealism in International Relations." In *Encyclopaedia of Power*, edited by K. Dowding, 332-33. Thousand Oaks: Sage, 2011.

Winder, D. "Iphone 13 Pro Hacked: Chinese Hackers Suddenly Break Ios 15.0.2 Security". *Forbes* (18 October 2021).

Winnefeld, J.A., P. Niblack, and D.J. Johnson. *A League of Airmen: Us Air Power in the Gulf War* Santa Monica RAND, 1994.

Wired-Staff-Writer. "Extreme Security Measures for the Extra Paranoid", *Wired*, 12 September 2019.

Wish, N.B. . "Foreign Policy Makers and Their National Role Conceptions". *International Studies Quarterly* 24, no. 4 (December 1989): 523-54.

Withers, P. . "What Is the Utility of the Fifth Domain?". *Air Power Review* 18, no. 1 (2015).

Wolff, J. "How Do We Know When Cyber Defenses Work? ". *Brooking Institute* (5 October 2022).

Wong, T. "China: What Does It Want from the Ukraine Crisis with Russia?", *BBC News* 4 February 2022.

Wood, R. . "Chinese Spy Ring 'Penetrating Taiwan Armed Forces'", *9 News* 22 December 2021.

Woodward, B. *Plan of Attack* New York: Simon and Schuster 2004.

Work, J.D. "China Flaunts Its Offensive Cyber Power ". *War on the Rocks* (22 October 2021).

World-Bank. "Military Expenditure (% of Gpd) – United Kingdom (2019)." https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS.

"World Economic League Table, 2021: A World Economic League Table". Centre for Economics and Business Research, 2020.

Wright, M. . "Western Values in International Relations." In *Diplomatic Investigations: Essays in the Theory of International Politics*, edited by H. Butterfield and M. Wight. London: Allen and Unwin, 1966.

Wright, T. "Putin Is Taking a Huge Gamble". *Brooking Institute* (10 December 2021).

Wrigley, C. *Churchill.* London: Haus, 2006.

Writer, Staff. "Biden Signs Enormous Us Military Budget into Law", *Al Jazeera*, 27 December 2021.

———. "Can China's J-20 Fighter Match up with America's F-35 Lightning Ii?". *The National Interest* (4 December 2021).

———. "China-Japan Hotline Launched to Avoid Sea, Air Clashes", *South China Morning Post* 8 June 2018.

———. "China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware". Medium.com, 2021.

———. "Companies Using Emc Rsa Securid": Enlytf 2022.

———. "'Defence Funding Boost 'Extends British Influence', Say Pm", *BBC News*, 19 November 2021.

———. "F-16 Fighting Falcon Multirole Fighter", *Air Force Technology*, 13 October 2021.

———. "F-35b: What You Need to Know About the Lightening Jet", *Forces.net* 17 November 2021.

———. "Field Marshal Montgomery – Obituary'", *New York Times*, 1976.

———. "Five Generations of Jets ", *Fighter World*, 2018.

———. "Hms Queen Elizabeth: All You Need to Know About the Aircraft Carrier." https://www.forces.net/news/hms-queen-elizabeth-all-you-need-know-about-britains-aircraft-carrier.

———. "Hms Queen Elizabeth: All You Need to Know About the Aircraft Carrier", *Forces.net*, 23 May 2021.

———. "Inauguration of Persian Gulf Air Defense Command Center", *YJC* 7 October 2019.

———. "Introduction: An Assessment of U.S. Military Power". *Heritage Foundation* (20 October 2021).

———. "Military Aircraft Market": Fortune Business Insights, 2021.

———. "Ngad: Usaf's Sixth Generation Fighter Is on Schedule, Aquisitions Officals Say", *Aero Space Manufacturing* 11 October 2021.

———. "Taiwan Gives up on F-35, Turns to F-16v Option". *The National Interest* (28 November 2018).

———. "Tensions in the East China Sea". *Council on Foreign Relations* (27 January 2022).

———. "Tiananmen Square: What Happened in the Protests of 1989?", *BBC News*, 23 December 2021.

———. "Us Carrier Transits Strait of Hormuz Amid Tensions with Iran", *AP*, 18 September 2020.

———. "Us Relations with China: 1949-2021". *Council on Foreign Relations* (10 December 2021 2021).

———. "Us Relations with Iran ". *Council on Foreign Relations* (30 December 2021).

———. "What Comes Next in the Standoff between the U.S. And Iran?". *World Politics REview* (31 January 2022 2022).

———. "What Is Rsa Securid?": Barracuda, 2021.

Writer, Stafff. "Who Are Taiwan’s Diplomatic Allies?", *Al Jazeera* 10 December 2021.

Wunische, A. . "Reviewing Why America Loses Wars". *The Strategy Bridge*, no. October (2019).

Yang, S. "200 Million Cyber Attacks Hit Taiwan's Military Networks in 2017", *Taiwan Times*, 28 May 2018.

Yeh, M., J. Jaworski, and S. Chase. "Pilot Perceptions on the Integration of Electronic Flight Bag Information in New Flight Deck Designs", In *Human Factors and Ergonomics Society Annual Meeting* 2019.

Yeo, M. "Taiwan Commissions First Upgraded F-16 Fighter Wing", *Defence News*, 19 November 2021.

———. "Taiwan Requests Fighter Jets from the Us, but with an Unusual Twist", *Defence News*, 11 March 2019.

Young, S. "Uk Set to Sign Contracts with Tempest Partners", *Reuters* 29 September 2021.

Yurdusev, A.N. . "Thomas Hobbes and International Relations: From Realism to Rationalism". *Australian Journal of International Affairs* 60, no. 2 (2006): 205-31.

Zapfe, M. . "Deterrence from the Groups Up: Understanding Nato’s Enhanced Froward Presence". *Survival* 59, no. 3 (2017): 147-60.

Zaranko, B. "Defence Funding Boost ‘Extends British Influence." By J. Bealse. *BBS News* (19 November 2020).

Zealand, New. "Defence Assessment: A Rough Sea Can Still Be Navigated ", edited by Ministry of Defence, 2021.

Zeidanloo, H. R., F. Tabatabaei, P.V. Amoli, and A Tajpour. "All About Malwares (Malicious Codes)". *Security and Management* (2010): 342-48.

Zetter, K. "Mossad Hacked Syrian Official’s Computer before Bombing Mysterious Facility", *Wired*, 11 March 2009.

———. "Russian 'Sandworm' Hack Has Been Spying on Foreign Governments for Years", *Wired* 14 October 2014 2014.

Zhang, B. . "The Perils of Hubris? A Tragic Reading of ‘Thucydides Trap’ and China-Us Relations". *Journal of Chinese Political Science* 2 (2019): 129-44.